004
V35

A 98

IOANA VASIU LUCIAN VASIU

DREPTUL TEHNOLOGIEI INFORMAȚIILOR ȘI COMUNICAȚIILOR

III 71.161

BIBL CENTR. UNIV
"M. EMINESCU" IASI
III 71.161

BCU IASI/CENTRAL UNIVERSITY LIBRARY

004
V35

Editura Albastră
Cluj-Napoca 2014

IOANA VASIU LUCIAN VASIU

7003821

DREPTUL TEHNOLOGIEI INFORMAȚIILOR ȘI COMUNICAȚIILOR

0 000010 29233 BCU IAȘI

BCU IASI / CENTRAL UNIVERSITY LIBRARY

ACU

Editura Albastră
Director editură
Smaranda Derveşteanu
Tehnoredactare computerizată
Editura Albastră
Coperta
Editura Albastră
Tipărit
Editura Albastră

12 DEC. 2014

Copyright © 2014
Toate drepturile asupra acestei lucrări aparţin s.c. Albastra Casă de Editură s.r.l. Reproducerea integrală sau parţială a textului sau a ilustraţiilor din această carte este posibilă numai cu acordul prealabil în scris al Casei de Editură Albastră.

BCU CLUJ CENTRAL UNIVERSITY LIBRARY

CUPRINS

1. TEHNOLOGIA INFORMAȚIILOR ȘI COMUNICAȚIILOR 5
1.1 Introducere 5
1.2 Cyberspațiul 6
1.3 Sisteme și date informatice 7
1.4 Componentele sistemelor informatice 13
1.5 Comunicații electronice 14
1.6 Internet 16

2. AFACERI ELECTRONICE 21
2.1 Aspecte introductive 21
2.2 Tipuri de afaceri 22
2.3 Modele de afaceri electronice 23
2.4 Cadrul legal privind tranzacțiile electronice 24
2.5 Tipuri de contracte electronice 30
2.6 Securitate informatică 31
2.7 Soluționarea litigiilor pe cale extrajudiciară 36
2.8 Restricții privind conținutul informațiilor furnizate 37
2.9 Instrument de plată electronică 38
2.10 Identificare electronică 43
2.10.1 Semnături electronice 44
2.10.2 Sigilii electronice 49
2.11 Marcarea temporală 50
2.12 Dispute privind numele de domeniu Internet 51
2.12.1 Cazuri privind mărci 59
2.12.2 Cazuri privind numele personale 66
2.12.3 Cazuri privind indicațiile geografice 68
2.12.4 Cazuri privind numele internaționale non-proprietar pentru substanțele farmaceutice 69

3. DREPTURI DE PROPRIETATE INTELECTUALĂ ÎN CYBERSPAȚIU 73
3.1 Cadrul legal internațional 75
3.2 Drept de autor și drepturi conexe 80
3.2.1 Protecția programelor informatice 80
3.2.1.1 Licențe informatice 81
3.2.1.2 Protecția tehnică 85
3.2.1.3 Protecția legală 87
3.2.2 Protecția operelor de artă digitală 90
3.2.3 Încălcarea drepturilor privind conținutul digital protejat 94
3.2.4 Managementul digital al drepturilor de autor 100

BCU IASI CENTRAL UNIVERSITY LIBRARY

3.3 Drepturi de proprietate industrială 105
3.3.1 Protecția semnelor distinctive 105
3.3.1.1 Mărci 105
3.3.1.2 Indicații geografice 112
3.3.2 Stimularea inovației și crearea de tehnologii 117
3.3.2.1 Brevet de invenție 117
3.3.2.2 Topografia produselor semiconductoare 122
3.3.2.3 Secrete comerciale 125
3.3.2.3.1 Cod sursă 130

4. INFRACȚIUNI INFORMATICE 137
4.1 Introducere 137
4.2 Hărțuirea electronică 140
4.3 Violarea vieții private 150
4.4 Fraude comise prin sisteme informatice și mijloace de plată electronice 160
4.4.1 Introducere 160
4.4.2 Frauda informatică 161
4.4.3 Efectuarea de operațiuni financiare în mod fraudulos 165
4.4.4 Acceptarea operațiunilor financiare efectuate în mod fraudulos 178
4.5 Falsul informatic 188
4.6 Infracțiuni contra siguranței și integrității sistemelor și datelor informatice 192
4.6.1 Introducere 192
4.6.2 Accesul ilegal la un sistem informatic 206
4.6.3 Interceptarea ilegală a unei transmisii de date informatice 218
4.6.4 Alterarea integrității datelor informatice 224
4.6.5 Perturbarea funcționării sistemelor informatice 228
4.6.6 Transferul neautorizat de date 236
4.6.7 Operațiuni ilegale cu dispozitive sau programe informatice 239
4.7 Pornografia infantilă 247

BCU IASI/CENTRAL UNIVERSITY LIBRARY

1. TEHNOLOGIA INFORMAȚIILOR ȘI COMUNICAȚIILOR

1.1 Introducere

Încă din cele mai vechi timpuri, reţelele au oferit oportunităţi pentru dezvoltare şi inovaţie şi au furnizat o structură pentru sistemele economice şi sociale. De la drumurile şi apeductele romane, până la sistemul de drumuri din secolul al XIX-lea şi la reţelele de sateliţi şi telecomunicaţii din zilele noastre, capacităţile oferite de reţele au fost folosite pentru a depăşi barierele de timp şi spaţiu şi pentru a deschide noi frontiere pentru interacţiunea şi activităţile umane[1]. Răspândirea largă a reţelele informatice are implicaţii majore asupra vieţii şi activităţii umane[2] şi a schimbat semnificativ societatea actuală. Cu excepţia electrificării, nici o altă invenţie tehnologică nu a afectat atât de fundamental modul în care oamenii trăiesc, lucrează, învaţă, comunică sau fac afaceri.

Sectorul tehnologiei informaţiilor şi comunicaţiilor contribuie foarte semnificativ la progresul tehnologic şi creşterea productivităţii[3]. Conform COM(2010) 245 final/2 (*O Agendă Digitală pentru Europa*), unul dintre pilonii strategiei Europa 2020, sectorul tehnologiei informaţiilor şi comunicaţiilor generează în mod direct 5% din PIB-ul european şi are o valoare de piaţă de 660 de miliarde euro anual. În SUA, pe de altă parte, în 2011, industria programelor şi a serviciilor informatice a generat venituri de 606 miliarde dolari[4].

Aplicaţiile tehnologiei informaţiilor şi comunicaţiilor sunt extrem de diverse, sistemele informatice devenind indispensabile în domenii esenţiale ale vieţii moderne: guvernare[5], financiar-bancar, industrial, educaţie, militar, televiziune, medical etc. Reţelele de comunicaţii electronice, în mod deosebit Internet, permit o inovaţie crescută[6], obţinerea de avantaje competiţionale[7],

---

1 Vezi R. J. Gordon, *Does the "New Economy" Measure up to the Great Inventions of the Past?*, NBER Working Paper No. w7833, 2000; J. S. Landefeld şi B. M. Fraumeni, *Measuring the New Economy*, Bureau of Economic Analysis, 2001; President's Information Technology Advisory Committee, *Information Technology Research: Investing in Our Future*, 1999.

2 Vezi H. C. Jr. Lucas, *Information technology and physical space*, Communications of the ACM, November, 44 (11), 89-96, 2001; OECD, *The new economy beyond the hype*, 2001.

3 Vezi OECD, *OECD Factbook*, 2013.

4 Vezi SelectUSA, *The U.S. Software and IT Services Industry*, n.d.

5 Vezi www.e-guvernare.ro; Ioana Vasiu şi Lucian Vasiu, *Top Management Skills in E-Government: A Conceptual Framework*, Journal of e-Government, 2 (3), 5-17, 2005.

6 Vezi E. Brynjolfsson, *The four ways IT is revolutionizing innovation*, MIT Sloan Management Review, 51, 3, Spring, 2010; OECD, *Information Technology Outlook*, 2010.

7 Vezi, spre exemplu, B. F. Kubiak şi M. F. Kowalik, *Marketing Information Systems as a Driver of an Organization's Competitive Advantage*, Journal of Internet Banking and Commerce, 15 (3), December, 2010; A. McAfee şi E. Brynjolfsson, *Investing in the IT That Makes a Competitive Difference*, Harvard Business Review, July, 2008; D.W. Jorgenson şi K. Motohashi, *Information Technology and the Japanese Economy*, NBER Working Paper No. 11801, 2005.

BCU CLUJ / CENTRAL UNIVERSITY LIBRARY

stocarea, procesarea şi transmiterea de cantităţi imense de date şi crearea de noi pieţe[8]. Sistemele informatice permit, de asemenea, reducerea timpului necesar şi a numărului de erori potenţiale cauzate de procesări manual, o mai bună gestionare a stocurilor, o utilizare intuitivă, adaptarea unor funcţii conform nevoilor utilizatorilor, posibilitatea de a colabora, cerceta (*virtual research communities*[9]) şi învăţa de la distanţă[10], de a integra sisteme şi aplicaţii diverse şi posibilitatea efectuării de tranzacţii financiare şi comerciale electronice sau mobile (cum ar fi *e-banking*, *m-banking*[11] sau *m-payment*[12]) prin folosirea de mesaje text (SMS) sau tehnologii precum *Wireless Application Protocol* (WAP), *Universal Subscriber Identity Module*[13] (USIM) sau *Near Field Communication* (NFC).

1.2 Cyberspaţiul

Cyberspaţiul este domeniul global în mediul informaţional, constând din reţeaua interdependentă de infrastructuri informatice, incluzând Internet, reţelele de comunicaţii electronice, sistemele informatice şi procesoarele şi controlerele incorporate[14]. Prin "reţea de comunicaţii electronice" se înţeleg sisteme de transmisie şi, după caz, echipamente de comutare sau de rutare şi alte resurse, inclusiv elemente de reţea care nu sunt active, care permit transmiterea semnalelor prin cablu, unde radio, prin mijloace optice sau prin alte mijloace electromagnetice, inclusiv reţele de satelit, reţele terestre fixe (cu comutare de circuite sau de pachete, inclusiv Internet) şi mobile, sisteme care utilizează reţeaua electrică, atât timp cât servesc la transmiterea semnalelor, reţelele utilizate pentru difuzarea programelor de radio şi televiziune şi reţelele de televiziune prin cablu,

---

8 Vezi, spre exemplu, J. D. Levin, *The Economics of Internet Markets*, NBER Working Paper No. 16852, 2011; Information Technology Industry Council, *The IT Industry's Cybersecurity Principles for Industry and Government*, 2011 (beneficiile globale anuale ale folosirii comerciale a Internetului sunt estimate la circa 1,5 trilioane dolari). Vezi şi A. Barua, P. Konana, A. B. Whinston şi F. Yin, *An Empirical Investigation of Net-Enabled Business Value*, MIS Quarterly, 28, 4, 585-620, 2004; T. Dewett şi G. R. Jones, *The Role Of Information Technology In The Organization: A Review, Model, And Assessment*, Journal of Management, 27, 3, 2001, p. 313 şi urm.; M. E. Porter, *Strategy and the Internet*, Harvard Business Review, March, 2001.

9 Vezi G. Andronico şi colab., *e-Infrastructures for e-Science: A Global View*, Journal of Grid Computing, Vol. 9 (2), 155-184, 2011.

10 Vezi, spre exemplu, C. Reimsbach-Kounatze, *Virtual Worlds: Immersive Online Platforms for Collaboration, Creativity and Learning*, OECD Digital Economy Papers, No. 184, 2011.

11 Spre exemplu, folosirea telefonului mobil pentru a deposita cecuri (*mobile remote deposit capture*): fotografiere faţă şi verso a cecului şi transmiterea imaginilor către instituţia bancară.

12 Vezi în T. R. McTaggart şi D. W. Freese, *Regulation of Mobile Payments*, The Banking Law Journal, Vol. 127, No. 6, June, 2010.

13 Aplicaţie care rulează pe un card cu cip (*Universal Integrated Circuit Card*) introdus într-un telefon mobil WCDMA 3G.

14 Vezi NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, 2011.

indiferent de tipul de informație transmisă[15]. Prin "rețea publică de comunicații" se înțelege o rețea de comunicații electronice utilizată, în întregime sau în principal, pentru furnizarea de servicii de comunicații electronice, puse la dispoziția publicului, care asigură transferul de informații între punctele terminale ale rețelei[16].

1.3 Sisteme şi date informatice

Expresia "**sistem informatic**" este interpretată diferit de numeroşii cercetători, comentatori, practicieni sau utilizatori ai acestora. Acest lucru se datorează faptului că domeniul sistemelor informatice este caracterizat drept un domeniu în fază timpurie de dezvoltare, afectat de inexactități conceptuale şi dezacorduri metodologice: o *adhocrație fragmentată*[17], care sugerează că domeniul ar fi în criză sau că s-ar îndrepta spre o criză[18]. Tradițional, un "sistem informatic" a fost definit prin două perspective: una referitoare la *funcția* sa, iar o a doua referitoare la *structura* sa.

Dintr-o perspectivă *structuralistă*, un "sistem informatic" constă dintr-o colecție de oameni, procese, date şi tehnologii care formează o structură care serveşte anumite funcții sau obiective. Pe de altă parte, dintr-o perspectivă *funcțională*, un sistem informatic este un mediu implementat tehnologic cu scopul de a înregistra, stoca şi transmite informații. Prin executarea acestor funcții, un sistem informatic facilitează crearea şi schimbul de înțelesuri care servesc scopuri sociale, cum ar fi executarea unor acțiuni, luarea unor decizii sau formularea sau justificarea unor idei.

Domeniul sistemelor informatice, domeniu crucial în activitatea contemporană, dar confuz[19], nu foloseşte un vocabular unificat, larg acceptat. Noțiunea de "sistem informatic" nu este definită în mod unic în literatura de specialitate[20] (de altfel, chiar noțiunea de "sistem" este definită diferit în literatura de specialitate) şi există diferite păreri privind domeniul sistemelor informatice: cât de larg sau cât de îngust este sau trebuie să fie acesta, precum şi ce discipline sunt legate de acest domeniu. După cum consideră Falkenberg şi colab.[21], în domeniul sistemelor informatice pot fi detectate cel puțin trei interpretări diferite:

---

15 Vezi Directiva 2009/140/CE a Parlamentului European şi a Consiliului din 25 noiembrie 2009 şi Legea nr. 527 din 17 iulie 2002.

16 *Id.*

17 Vezi J. Rose, *Information systems development as action research - soft systems methodology and structuration theory*, Ph.D. Thesis, 2000.

18 Vezi H. K. Klein şi R. Hirschheim, *Crisis in the IS Field? A Critical Reflection on the State of the Discipline*, Journal of the AIS, 4, November, 2003.

19 Vezi P. Checkland şi S. Holwell, *Information, Systems, Information Systems – Making sense of the field*, John Wiley & Sons, 1998.

20 Vezi Steven Alter, *Defining information systems as work systems: implications for the IS field*, European Journal of Information Systems, 17, 448–469, 2008.

21 Vezi E. D. Falkenberg, Hesse, W., Lindgreen, P., Nilsson, B. E., Oei, J. L. H., Rolland, C., Stamper, R. K., Van Assche, F. J. M., Verrijn-Stuart, A. A. şi K. Voss, *A framework of information system concepts*, The FRISCO Report, 1998.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

- Abordarea ca *sistem tehnic*, implementat cu calculatoare şi tehnologia telecomunicaţiilor;
- Abordarea ca *sistem social* (o organizaţie cu nevoi informaţionale);
- Abordarea ca *sistem conceptual* (adică, o abstracţie a uneia dintre cele de mai sus).

Falkenberg şi colab.[22] consideră subsecvent că trebuie să acceptăm că există multe subdomenii diferite, care privesc diverse seturi de probleme, unde se găsesc cuvinte cum ar fi informaţie, dată, comunicare, proces, cunoaştere, sistem etc., cu înţeles local, restrâns, neîmpărtăşit pe scară largă. Pe lângă natura interdisciplinară a domeniului sistemelor de informaţii, se subliniază existenţa a trei surse majore de probleme:

- Marea varietate a grupurilor de interese,
- Poziţiile filozofice conflictuale[23] şi
- Lipsa unei înţelegeri precise a comunicărilor.

Un "sistem informatic" este, în general, considerat a fi un sistem compus din utilizatori, date, tehnologii şi procese, care permite colectarea, stocarea, procesarea şi comunicarea informaţiei intra- sau inter-organizaţional[24]. Goldin şi colab.[25] consideră că un "sistem informatic" este un termen generic ce se referă la *sisteme software*, care furnizează servicii bazate pe informaţii. O definiţie sintetică este propusă de Christie şi Christie: "într-o organizaţie, întreaga colecţie de proceduri, operaţii şi funcţii dedicate generării, colectării, evaluării, stocării şi diseminării datelor şi informaţiilor"[26].

Palmius[27], pe de altă parte, consideră că un "sistem informatic" (*information system*) este ansamblul elementelor care păstrează informaţii, canalelor capabile să distribuie informaţii şi actorilor care acţionează pe baza informaţiei, refuzând o definiţie care exclude oamenii ca fiind *parte* a unui sistem informatic. O abordare asemănătoare oferă Rose, pentru care un "sistem informatic" include echipament (componente *hardware*), programe informatice (componente *software*) şi sistemul social care *orchestrează* furnizarea organizată a informaţiei, cele două formând o reţea socio-tehnică[28]. Sawyer[29] extinde înţelegerea conceptului şi consideră că într-un "sistem informatic" programele informatice (*software*) reprezintă componenta principală, sistemul incluzând şi

---

22 Vezi E. D. Falkenberg şi colab., op. cit.

23 Vezi şi G. Walsham, *Interpreting information systems in organisations*, 1993.

24 Vezi K. C. Laudon şi J. P. Laudon, *Essentials of Management Information Systems, Transforming Business and Management*, 3rd Edition, Prentice Hall, 1999.

25 Vezi D. Goldin, B. Thalheim şi S. Srinivasa, *Information systems = Databases + Interaction: Towards principles of information system design*, 2000.

26 Vezi Linda Gail Christie şi John Christie, *The Encyclopedia of Microcomputer terminology*, Prentice Hall, 1984.

27 Joel Palmius, *Defining the "Information" Part of "Information System"*, Proceedings of the 28th Information Systems Research Seminar in Scandinavia, 2005.

28 Vezi J. Rose, op. cit.

29 Vezi S. Sawyer, *A market-based perspective on information systems development*, Communications of the ACM, November, 44 (11), 2001, p. 97-102.

BUCHAREST UNIVERSITY LIBRARY

echipament (*hardware*), oameni (utilizatori, administratori, manageri) şi *reguli*, care permit programelor pentru calculator să lucreze pentru a servi utilizatorii, dar este atent să puncteze că distincţia între programe informatice şi sisteme informatice evidenţiază celelalte componente, care trebuie asamblate pentru a crea un *sistem funcţional*.

Nici definiţiile legale nu oferă o înţelegere unitară a "sistemului informatic". Astfel, conform Codului penal din Texas (Sec. 33.01), prin "sistem informatic" (*computer system*) se înţelege orice combinaţie de calculatoare sau reţele de calculatoare cu documentaţie, programe informatice (*computer software*) sau facilităţi fizice care suportă calculatoare sau reţele informatice. Conform Codului penal al statului California (Section 502), prin "sistem informatic" (*computer system*) se înţelege un dispozitiv sau o colecţie de dispozitive, unul sau mai multe dintre acestea conţinând programe informatice, instrucţiuni electronice, date de intrare şi ieşire, care execută un număr de funcţii, printre acestea funcţii logice, aritmetice, de stocare şi accesare date, comunicare şi control.

Conform art. 1 (a) al Convenţiei Consiliului Europei asupra criminalităţii informatice[30], prin "sistem informatic" (*computer system*) se înţelege orice dispozitiv sau grup de dispozitive interconectate sau relaţionate, unul sau mai multe dintre acestea, conform unui program informatic, executând procesarea automată a datelor. Un asemenea sistem poate include intrări, ieşiri sau capacităţi de stocare de date, poate funcţiona singur sau poate fi conectat la o reţea sau la alte dispozitive similare.

Definiţiile date de noul Cod penal în Art. 181 conceptelor de "sistem informatic" şi, respectiv, de "date informatice" sunt identice cu cele date de legiuitorul român în art. 35 (1) din Legea nr. 161/2003 şi identice cu cele date de legiuitorul european în Cybercrime Convention (Cap. I, art. 1, lit. a): prin "sistem informatic" se înţelege "orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie funcţională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic". Prin "date informatice" se înţelege "orice reprezentare a unor fapte, informaţii sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic".

Prevederile din art. 181 nu au un corespondent în vechiul Cod penal, fiind preluate din Legea nr. 161/2003, lege privitoare la unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei, publicată în M. Of. nr. 275 din 21 aprilie 2003, Titlul III, *Prevenirea şi combaterea criminalităţii informatice*, art. 35, alin. 1, lit. a) şi d). Aceste definiţii fuseseră preluate şi în noul Cod penal abrogat (Legea nr. 301/2004), diferenţa dintre aceste două noi coduri penale în această privinţă este aceea că în timp ce noul Cod penal din 2004 prelua toate definiţiile date de Legea nr. 161/2003 la art. 35 (1), noul Cod penal din 2009 nu preia decât aceste două definiţii: "sistem informatic" şi "date informatice".

Sursa de inspiraţie pentru aceste definiţii este Convenţia Europeană privind criminalitatea informatică (*Cybercrime Convention*) din 2001, intrată în vigoare în

[30] Vezi Council of Europe, *Convention on Cybercrime*, European Treaty Series No. 185, 2001, disponibilă la locaţia http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.

B.C.U. „M. EMINESCU" IAŞI

august 2004, semnată şi ratificată de ţara noastră. La nivel european, aceşti termeni au o definire unitară, având în vedere faptul că, în Raportul Explicativ al Convenţiei, termenii ce apar în definirea infracţiunilor informatice sunt foarte clar detaliaţi. Legiuitorul european în Raportul Explicativ al Convenţiei[31] a detaliat definiţia conceptului de "sistem informatic" şi cea a conceptului de "date informatice" după cum urmează: un "sistem informatic" (computerizat) este *un dispozitiv compus din echipament şi programe informatice, realizat pentru procesarea automată (fără intervenţie umană directă) a datelor (datele din sistemul computerizat sunt operate prin executarea unui program informatic, adică a unui set de instrucţiuni care pot fi executate de calculator pentru obţinerea rezultatului dorit). Un calculator poate rula diferite programe informatice şi poate consta din diferite periferice, distincte faţă de unitatea centrală de procesare şi periferice (dispozitiv care poate executa diferite funcţii specifice în interacţiune cu unitatea centrală, cum ar fi o imprimantă, ecran video sau cititor/inscriptor de CD-uri).*

În Directiva 2013/40/EU a Parlamentului European şi a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice şi de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului, legiuitorul european preferă următoarea definiţie, mai complexă prin cuprinderea datelor informatice ca parte a unui "sistem informatic": "un dispozitiv sau grup de dispozitive interconectate sau omoloage, dintre care unul sau mai multe asigură, prin intermediul unui program, prelucrarea automată a datelor informatice, precum şi datele informatice stocate, prelucrate, recuperate sau transmise de acest dispozitiv sau grup de dispozitive în vederea exploatării, a utilizării, a protecţiei şi a întreţinerii lor".

În general, prin "dată" se înţelege un set de fapte discrete despre evenimente sau lumea înconjurătoare. "**Dată informatică**" este orice simbol sau semn care este într-o formă ce poate fi stocată digital. Conform Christie şi Christie, prin "date informatice" înţelegem numere, litere, simboluri sau fapte care descriu un obiect, idee, condiţie, situaţie sau alt factor, acestea fiind elemente de bază ale informaţiei, care pot fi procesate sau produse de un calculator[32]. Chiar dacă datele şi instrucţiunile pot avea aceeaşi formă sau expresie, o distincţie funcţională există între ele.

Conform art. 1 (b) al Convention on Cybercrime prin "date informatice" se înţelege orice reprezentare de fapte, informaţii sau concepte într-o formă adecvată procesării într-un sistem informatic, incluzând un program informatic care poate determina executarea unei funcţii de către un sistem informatic. Directiva 2013/40/UE a Parlamentului European şi a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice şi de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului, defineşte conceptul de "date informatice" ca fiind o reprezentare de fapte, informaţii sau concepte, într-o formă adecvată pentru prelucrare într-un sistem informatic, inclusiv un program, care permite unui sistem informatic să execute o funcţie. În Raportul explicativ, legiuitorul european a dorit

---

[31] Vezi Council of Europe, *Explanatory Report to the Convention on Cybercrime*, 2001.
[32] Vezi Linda Gail Christie şi John Christie, op. cit.

BCU IAŞI / CENTRAL UNIVERSITY LIBRARY

şi mai multă claritate în înţelegerea acestui concept, astfel că a făcut următoarele precizări: expresia "apte de a fi procesate" trebuie interpretată în sensul că datele se află într-o anumită formă, care poate fi în mod direct procesată de un sistem computerizat; datele informatice sunt date în formă electronică sau într-o altă formă, care asigură procesarea lor directă.

Principalele atribute ale datelor informatice se referă la *confidenţialitate*, *integritate* şi *disponibilitate*. Alături de aceste atribute esenţiale, Parker[33] discută şi *utilitatea*, *posesia*, *locaţia* ş.a., alţi autori adaugând şi alte cerinţe de securitate, cum ar fi *folosirea legitimă*[34].

Confidenţialitatea este un atribut care se referă la *date* informatice şi vizează prevenirea accesului fără drept la date informatice. Datele informatice pot avea o valoare economică importantă, ceea ce poate duce la atacuri informatice care vizează accesul neautorizat la acestea, implicit încălcarea confidenţialităţii lor. Datorită caracteristicilor sistemelor informatice[35], atacurile care vizează încălcarea confidenţialităţii datelor informatice sunt, în unele situaţii, dificil de detectat sau contracarat.

Încălcarea confidenţialităţii datelor personale, spre exemplu, poate avea multiple consecinţe nefaste pentru cei afectaţi[36]. Persoanele care accesează fără autorizarea proprietarului un sistem informatic, sau care depăşesc autorizarea pe care o au şi accesează date informatice protejate, violează dreptul legitim al proprietarului de a proteja acele date împotriva accesului. Confidenţialitatea priveşte şi controlul accesului la opere stocate în formă digitală[37]. Confidenţialitatea poate fi un aspect foarte important în cazul secretelor militare sau comerciale[38] sau pentru respectarea unor cerinţe legale (cum ar fi, spre exemplu, nediseminarea dosarelor medicale sau comunicaţiilor avocat-client).

Deoarece violarea confidenţialităţii datelor informatice presupune acces la un sistem informatic[39], "accesul ilegal" este considerat o infracţiune de bază în

---

33 Vezi D. B. Parker, *Fighting computer crime: A new framework for the protection of information*, 1999.

34 Vezi, spre exemplu, C. E. Landwehr, *Computer security*, International Journal of Information Security, 1, 3–13 (2001); D. Amor, *The E-Business (R)evolution: Living and Working in an Interconnected World* (2nd Ed.), Prentice Hall, 2001.

35 Avem în vedere aici, printre altele, dificultăţile inerente de securizare a datelor informatice, posibilitatea ca datele să se afla în posesia deţinătorilor legitimi chiar şi după ce au fost accesate sau copiate şi dificultăţile privind discriminarea acţiunilor legitime de cele ilegitime.

36 Dreptul la protecţia datelor personale este inerent *dreptului la libertate* şi noţiunilor de *încredere* şi *respect* - vezi opinia exprimată în C. Fried, *Privacy*, 77 Yale Law Journal, 1968, p. 477-478. Datele personale pot fi senzitive (spre exemplu, date financiare sau medicale), în unele cazuri asemenea date fiind copiate sau divulgate către terţe părţi, cu consecinţe serioase pentru cei afectaţi - vezi cazuri reale în L. R. Mizell, *Invasion of Privacy*, Berkeley Books,1998.

37 Vezi, spre exemplu, Ioana Vasiu şi Lucian Vasiu, *Un cadru holohedral pentru protejarea tehnică a proprietăţii intelectuale digitale*, Revista Română de Dreptul Proprietăţii Intelectuale, Nr. 1 (6), 138-143, 2006; D. L. Burk şi J. E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, Harvard Journal of Law and Technology, 15, 2001.

38 Informaţiile pot fi considerate "secret comercial" numai dacă nu sunt larg cunoscute şi măsuri de securitate rezonabile au fost implementate pentru păstrarea confidenţialităţii.

39 Vezi o abordare interesantă a controlului accesului în E. Bertino, B. Catania, E. Ferrari şi P. Perlasca, *A logical framework for reasoning about access control models*, ACM Transactions

cadrul infracțiunilor săvârșite cu ajutorul calculatorului[40]. Confidențialitatea poate avea mai multe nivele, pornind de la restricționarea citirii, imprimării sau transmiterii datelor informatice și mergând până la restricționarea informațiilor privind existența unor date informatice[41].

Integritatea se referă la păstrarea corectă, nealterată și completă a *datelor* informatice[42]. Integritatea datelor informatice are atât componente fizice, cât și componente logice și implică anumite condiții dezirabile, care sunt menținute în timp, referitoare la menținerea sau păstrarea datelor în condiții corespunzătoare situației inițiale sau care reflectă fapte corecte[43]. În cazul bazelor de date, integritatea vizează date, metadate și funcții.

Nivelul de senzitivitate variază în funcție de domeniu și de circumstanțe, mergând de la toleranță zero la orice fel de modificări (doarece chiar modificări minore ale datelor informatice pot afecta dramatic statutul legal sau consecințele procesări unor asemenea date), până la o anumită toleranță față de modificarea datelor[44]. Integritatea este, de asemenea, o cerință legală: dacă una dintre părți are nevoie să dovedească ceva, primul lucru care trebuie făcut este probarea integrității înregistrărilor (stocate pe un suport fizic) respectivei tranzacții sau comunicații, pentru ca o instanță judecătorească să o considere o dovadă credibilă.

Disponibilitatea *datelor* sau *sistemelor* informatice se referă la prevenirea acțiunilor care împiedică sau întârzie semnificativ accesul legitim la date sau folosirea legitimă a sistemelor informatice. Printre asemenea acțiuni se numără criptarea[45], ștergerea datelor și atacurile care vizează refuzul serviciului (atacurile de tip *Distributed Denial-of-Service* - DDoS). Atacurile de tip DDoS consumă resursele unui sistem informatic, resurse destinate servirii utilizatorilor legitimi.

Există două subcategorii principale de atacuri în această categorie: atacuri logice și atacuri de "inundare" (*flooding attacks*). În aceste atacuri, sunt adesea folosite *botnets*, care constau din sute sau chiar mii de calculatoarele compromise, infectate în prealabil și controlate de la distanță, transformate într-un grup de

---

on Information and System Security, 6, 71 – 127, 2003.

40 Vezi detalii în M. Goodman, *Making computer crime count*, FBI Law Enforcement Bulletin, August, 2001, p. 10-17.

41 Vezi C. P. Pfleeger, *Security in Computing*, Addison Wesley (1997).

42 Vezi definiții în Ravi S. Sandhu, *On Five Definitions of Data Integrity*, Proc. of the IFIP WG11.3 Workshop on Database Security (1993)

43 Vezi P. G. Neumann, *Computer related risks*, 1995; Ioana Vasiu și Lucian Vasiu, *Break on Through: An Analysis of Computer Damage Cases*, Pittsburgh Journal of Technology Law & Policy, Vol. XIV, Spring, p. 158-201, 2014.

44 Vezi C. P. Pfleeger, op. cit., p. 333.

45 Vezi cazul GpCode, care suprascrie fișiere cu date criptate, care nu pot fi recuperate fără cheia privată folosită (în acest caz, AES cu chei de 256 biți și RSA cu chei de 1024 biți, care nu permit decriptarea într-un interval de timp rezonabil), descris de Kaspersky Lab, *IT Threat Evolution for Q1-2011*. Vezi și Enargy Power Co. Ltd. v. Wang, Civil Action No. 13-11348-DJC (D. Mass. Dec. 3, 2013).

calculatoare "zombi". Aceste atacuri sunt foarte periculoase deoarece sunt foarte dificil de contracarat[46].

1.4 Componentele sistemelor informatice

Componentele *tehnologice* ale unui sistem informatic pot fi clasificate după cum urmează:

- Calculatoare (*hardware*);
- Programe informatice (*software*);
- Periferice [de intrare (*input*), de ieşire (*output*) şi de stocare];
- Legături de comunicaţii.

Un **calculator** este un sistem fizic care prelucrează datele introduse într-o formă prestabilită şi furnizează rezultate, fie într-o formă accesibilă utilizatorului, fie ca semnale destinate acţionării unor echipamente[47] (altfel spus, o maşină capabilă să efectueze automat operaţii aritmetice şi logice, cu scopuri ştiinţifice, administrative, contabile etc., plecând de la programe care definesc secvenţa acestor operaţii)[48]. Calculatoarele au o componentă de *echipament* (*hardware*) şi un set de *programe* informatice (*software*).

Calculatoarele conţin un număr de subsisteme. Un calculator poate fi văzut, din punct de vedere al echipamentului, ca un sistem constând din 5 subsisteme funcţionale: intrare (*input*), control, procesare aritmetică şi logică, memorie şi ieşire (*output*). Calculatoarele pot fi calculatoare personale (de birou sau portabile), console pentru jocuri video, staţii de lucru (*workstations*), server-e, *mainframes* şi supercalculatoare.

Printr-un **program informatic**, se înţelege o colecţie de instrucţiuni pentru calculator, proceduri şi documentaţie, vizând realizarea uneia sau mai multor acţiuni pe un sistem informatic. Expresia include *programe de aplicaţie* (spre exemplu, procesoare de texte sau programe pentru calcul tabelar), *sisteme de operare* şi *middleware* (programe care controlează şi coordonează sisteme distribuite)[49]. Un "program informatic" este o secvenţă de *instrucţiuni*, scrise într-un anumit limbaj de programare, într-o anumită ordine, care spune calculatorului *ce* să facă.

Programele informatice pot fi incorporate în topografia circuitelor sau pot exista sub formă de *cod sursă* sau *cod obiect*. Ciclul de dezvoltare al programelor informatice cuprinde următoarele faze: studiu de fezabilitate, formularea sau definirea cerinţelor, design, implementare, integration şi testare, întreţinere. Vulnerabilitatea programelor informatice[50] sau prezenţa erorilor de programare (*bug*-uri)[51] pot afecta serios calitatea sistemelor informatice[52].

---

[46] A se vedea o discuţie detaliată şi cazuri în care disponibilitatea datelor sau sistemelor informatice a fost afectată în Ioana Vasiu şi Lucian Vasiu, *Break on Through: An Analysis of Computer Damage Cases*, op. cit.

[47] Vezi *Dicţionar de informatică*, Ed. Ştiinţifică şi Enciclopedică, Bucureşti, 1981.

[48] Conform *Dictionnaire de notre temps*, Hachette, Paris, 1988.

[49] Vezi şi definiţia WIPO, *Model Provisions on the Protection of Computer Software*, 1977.

[50] Vezi, spre exemplu, J. J. Pauli şi D. Xu, *Misuse Case-Based Design and Analysis of Secure Software Architecture*, Proceedings of the International Conference on Information

Atacurile asupra programelor informatice pot viza:

- ***Modificarea codului*** (*tampering attack*), în care atacatorul violează integritatea unui program informatic;
- ***Dezasamblarea malițioasă*** (*malicious reverse-engineering attack*), în care atacatorul violează drepturile de confidențialitate ale titularului drepturilor de autor (algoritmi, design sau implementare);
- ***Clonarea*** (*cloning attack*), în care atacatorul violează drepturi de proprietate intelectuală prin fabricarea și distribuirea de copii ilegale ale unui program informatic. Ataccurile informatice pot viza n modificarea codului unui program (*client code*)[53]. Metodele de protejare împotriva unor asemenea atacuri vizează detectarea modificărilor și repararea programelor afectate[54].

1.5 Comunicații electronice

În orice comunicație distingem:

- *Transmițătorul* - persoana sau dispozitivul capabil să transmită un mesaj;
- *Receptorul* (destinatarul) - persoana sau dispozitivul capabil să recepționeze un mesaj;
- *Mediul de transmisie* - mijlocul prin care se transmite mesajul, informația (spre exemplu, un cablu);
- *Informația* - ceea ce se transmite (mesajul, datele);
- *Zgomotul* - mijlocul fizic ce interferează cu procesul de comunicare.

Există două moduri de transmisie codificată a informației: în *paralel* și în *serie* (în cadrul acestei transmisii, există trei moduri de transmisie: *asincronă*, *sincronă* și *izocromă*). Pentru a facilita comunicațiile electronice, calculatoarele sunt legate în *rețele informatice* (rețele de calculatoare).

Rețele informatice

O rețea informatică rezultă din interconectarea a două sau mai multe sisteme informatice. Interconectarea poate fi comună (*eartbound*), prin fire sau cabluri, *wireless*-prin radio, infraroșii sau satelit, sau ambele. Rețeaua poate fi limitată din

---

Technology: Coding and Computing, 2005; P. G. Neumann, *Computer-Communications Security Risks: Melissa is Just the Tip of a Titanic Iceberg*, Written testimony for the U.S. House Science Committee Subcommittee on Technology, 1999.

51 Vezi, spre exemplu, E. W. Dijkstra, *The end of computing science?*, Communications of the ACM, 44 (3), March, 92, 2001.

52 De remarcat existența unor utilitare care permit depistarea erorilor de programare, cum ar fi, spre exemplu, *Advanced Combinatorial Testing System*, dezvoltat de NIST, care permite găsirea eficientă a erorilor în programe informatice - vezi *Testing Tool Finds Software Bugs Efficiently*, Computer, Feb, 15, 2011.

53 Vezi M. Ceccato și P. Tonella, *CodeBender: Remote Software Protection Using Orthogonal Replacement*, IEEE Software, 2011.

54 Vezi P. Falcarin, C. Collberg, M. Atallah și M. Jakubowski, *Software Protection*, IEEE Software, March-April, 2011.

punct de vedere geografic la o zonă restrânsă (*local area network*) sau se poate întinde pe o suprafaţă mare (*wide area networks*). Sistemele informatice pot fi conectate la reţea ca "puncte finale" (*endpoints*) sau ca mijloace de asistenţă în comunicaţia din reţea.

Într-o reţea informatică, există cel puţin un *file server* (calculator central, care păstrează pe discul său dur fişierele utilizate de celelalte calculatoare legate în reţea) şi un număr de calculatoare conectate la reţea, numite "clienţi" (*clients*), "terminale" (*terminals*) sau "staţii" (*stations*). Există un număr de avantaje care îndreptăţesc legarea calculatoarelor în reţele: posibilitatea partajării resurselor (spre exemplu, discuri dure sau imprimante), fişierele de date sau anumite programe pot fi stocate pe un calculator central etc.

Reţelele informatice pot fi clasificate după cum urmează:

- Locale (*Local-Area Network* - LAN): Calculatoarele la distanţă mică unele de altele, de regulă în aceeaşi clădire;
- La nivel extins (*Wide-Area Network* - WAN): Calculatoarele sunt la distanţă unele de altele, conectate prin linii telefonice sau unde radio;
- La nivel campus (*Campus-Area Network* - CAN): Calculatoarele sunt într-o zonă restrânsă, cum ar fi un campus sau o bază militară;
- La nivel metropolitan (*Metropolitan-Area Network* - MAN): Calculatoarele sunt plasate la nivel de oraş;
- La nivel domiciliu (*Home-Area Network* - HAN): Calculatoarele sunt situate în locuinţa unei persoane.

Cele mai cunoscute **protocoale** de reţea sunt IP (Internet Protocol), UDP (User Datagram Protocol), TCP (Transmission Control Protocol), DHCP (Dynamic Host Configuration Protocol), HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), Telnet (Telnet Remote Protocol), SSH (Secure Shell Remote Protocol), POP3 (Post Office Protocol 3), SMTP (Simple Mail Transfer Protocol), IMAP (Internet Message Access Protocol), SOAP (Simple Object Access Protocol), PPP (Point-to-Point Protocol). **Conexiunile de bandă largă** pot fi de tip: *Digital Subscriber Line* (bazată pe transmisie prin linii telefonice tradiţionale; această conexiune poate fi de tip ADSL, SDSL, HDSL sau VSDL); Modem (furnizată prin cablu coaxial); Fibră optică; *Wireless* (bazată pe o legătură radio între locaţia clientului şi cea a furnizorului); Satelit; *Broadband over Powerlines* (furnizată prin intermediul retelelor electrice).

Modelul de reţea ISO

Reţelele informatice sunt adesea descrise în termenii modelului Open Systems Interconnection (OSI) Reference Model, folosit de International Organization for Standardization (ISO), identificat ca ISO/IEC 7498-1. Acest model constă în 7 nivele privind programele şi/sau echipamentul informatic, fiecare reprezentând un nivel de abstracţie. La cel mai jos nivel, modelul specifică modul în care echipamentul transmite informaţia prin reţea, în timp ce nivelle înalte privesc aspecte cum ar fi fiabilitatea, securitatea sau independenţa de echipament a datelor. Tabelul 1 prezintă modelul ISO/OSI.

Tabel 1. Modelul ISO/OSI.

Nivel	Nume	Funcţie
1	Fizic	Cablul sau mediul fizic
2	Date	Transmite/primeşte pachete, identifică adrese hardware
3	Reţea	Determină rutarea şi contabilizează
4	Transport	Garantează transfer corect al datelor
5	Sesiune	Autentificare şi autorizare
6	Prezentare	Aspecte privind datele şi compresia acestora
7	Aplicaţie	Servicii pentru utilizatorul final

TCP/IP

TCP/IP (*Transmission Control Protocol/Internet Protocol*), numit şi *modelul Internet*, este un set de protocoale de comunicaţii întreţinut de Internet Engineering Task Force (IETF) şi folosit pe Internet şi în reţele de calculatoare similare. TCP/IP nu presupune nici un echipament sau program specific, ceea ce permite implementarea sa pe orice platformă. TCP/IP permite conectivitate de tip *end-to-end*, specificând modul în care datele trebuie adresate, transmise şi receptate la destinaţie. Această funcţionalitate este organizată în următoarele nivele: Legătură (*Link* sau *Network interface layer*), care permite interfaţa cu echipamentul de reţea; Reţea (*Internetwork, Network* sau *Internet layer*); Transport (*Transport layer*), care permite transferul de date *end-to-end* prin transmiterea datelor de la o aplicaţie la alta; Aplicaţie (*Application layer*), furnizat de programul care foloseşte TCP/IP pentru comunicare. Tabelul 2 prezintă modelul TCP/IP.

Tabel 2. Modelul de reţea TCP/IP.

Nivel	Funcţie
Legătură	Echipament reţea şi *driver*-e pentru acestea
Reţea	Comunicaţii de bază, adresare şi rutare
Transport	Comunicare între programe
Aplicaţie	Programe pentru utilizatorul final (permite unei aplicaţii transmiterea şi primirea de date)

1.6 Internet

Internet este "reţeaua de reţele informatice", sau mulţimea de calculatoare şi facilităţi de telecomunicaţii, incluzând echipament şi programe informatice, conectate prin tehnologii electronice, fără fir (*wireless*) şi optice care folosesc protocolul TCP/IP, sau orice precedesor sau succesor al acestui protocol, pentru a comunica informaţii de orice tip. Internet constă din *Reţele mari*, numite *backbones*, ale unor entităţi comerciale şi care au ca scop interconectarea altor reţele [acestea mai sunt numite şi *Network Access Points* (NAPs) sau *Internet Exchange Points* (IXPs)]; *Reţele regionale*, care conectează alte reţele, cum ar fi cele

BCU IASI / CENTRAL UNIVERSITY LIBRARY

ale universităţilor; *Reţele comerciale*, care furnizează acces abonaţilor la *backbones*; şi *Reţele locale*.

În funcţionarea Internetului, un rol esenţial este jucat de *sistemul numelor de domeniu* (DNS)[55]. În vârful ierahiei sistemului numelor de domeniu se găseşte zona rădăcină (*root zone*), care conţine informaţii referitoare la domeniile de nivel de vârf (*top-level domains* sau TLDs). Zona rădăcină este publicată prin intermediul unui sistem distribuit de servere de nume de domeniu numite servere rădăcină (*root servers*). Modificările informaţiei din zona rădăcină sunt autorizate de U.S. Department of Commerce, conform termenilor contractului cu The Internet Corporation for Assigned Names and Numbers (ICANN[56]), privind funcţiile Internet Assigned Numbers Authority (IANA[57]). Modificările zonei sunt distribuite conform the Cooperative Research and Development Agreement (CRADA) între VeriSign şi U.S. Department of Commerce[58].

Fiecare domeniu Internet are un nume, care serveşte drept referinţă mnemonică la o anumită combinaţie de numere asignată unui calculator în reţea, având rolul de a facilita utilizatorilor găsirea locaţiilor pe Internet. Avantajul real al sistemului numelor de domeniu este acela că împarte gigantica lume Internet în bucăţi administrabile. Numele sunt organizate într-un mod raţional, uşor de înţeles, astfel încât sunt relativ uşor de reţinut numele utile.

Uniform Resource Locator sau *Universal Resource Locator* (URL), definit în 1994 de RFC 1738, este un şir de caractere care specifică unde se găseşte o anumită resursă pe Internet şi mecanismul de găsire a acesteia. Fiecare URL constă dintr-un nume de schemă (protocol), caracterul ":", două caractere "/", un nume de domeniu sau o adresă IP, un număr de port, calea către resursa dorită sau programul care se doreşte executat, apoi, pentru programe cum ar fi scripturi Common Gateway Interface (CGI), un şir de caractere şi un identificator de fragment.

Sistemul numelor de domeniu (DNS) permite utilizatorilor referirea locaţiilor web prin nume uşor de reţinut, în loc de folosirea de adrese IP numerice. O adresă IP este formată din 4 octeţi (*bytes*) şi este divizată într-o parte de reţea şi una *host*. Partea de reţea identifică reţeaua logică la care se referă adresa, deciziile de rutare fiind bazate pe această informaţie)[59]. Partea *host* indică un anumit calculator în cadrul respectivei reţele[60]. Versiunea IPv4, activă din 1983, foloseşte

---

[55] Numele de domeniu (*domain name*) reprezintă, de fapt, o adresă în Internet. Pentru a scuti utilizatorii de efortul introducerii de la tastatură a unor numere dificil de reţinut, Internet a fost organizat ca o colecţie de domenii. Sistemul numelor de domeniu a fost inventat în 1983, specificaţiile originale apărând în publicaţiile RFC 882 şi RFC 883, fiind modificat ulterior (spre exemplu, în noiembrie 1987, în publicaţiile RFC 1034 şi RFC 1035).

[56] Vezi detalii la http://www.icann.org.

[57] Vezi detalii la http://www.iana.org.

[58] https://www.icann.org/resources/unthemed-pages/crada-report-summary-2003-03-14-en

[59] Atacurile asupra furnizorilor de servicii DNS pot rezulta în redirectări către site-uri contrafăcute (*Pharming*). Vezi, spre exemplu, cazul furnizorilor NetNames şi Ascio, care a afectat circa 200 de site-uri web proeminente, utilizatorii care încercau să le viziteze au fost redirectaţi către un site al atacatorilor – vezi SANS, *NewsBites*, Vol. XIII, Iss. 71, September 06, 2011. Vezi şi viermele Koobface ca *DNS changer* şi atacurile de tip *DNS Poisoning* (executarea de cod maliţios pe un server DNS server pentru redirectări web).

[60] Vezi E. Nemeth şi colab., *UNIX System Administration Handbook*, Prentice Hall, 1995.

numere de 32 de biţi şi a permis existenţa a peste 4 miliarde de adrese de acest tip. Clasa unei adrese poate fi determinată prin examinarea primului octet. Tabelul 3 descrie clasele şi caracteristicile acestora (porţiunea de reţea este denotată de 'N', iar cea *host* de 'H').

Tabel 3. Clasele de adrese Internet.

Clasă	Primul octet[61]	Format
A	1-126	N.H.H.H
B	128-191	N.N.H.H
C	192-223	N.N.N.H
D	224-239	-
E	240-254	-

IANA alocă resurse Internet către *Regional Internet Registries*, organizaţii care administrează alocarea şi înregistrarea numerelor Internet într-o anumită zonă a globului: AfriNIC (www.afrinic.net) pentru Africa; APNIC (www.apnic.net) pentru Asia/Pacific; ARIN (www.arin.net) pentru America de Nord; LACNIC (www.lainic.net) pentru America latină şi unele insule din Caraibe; RIPE NCC (www.ripe.net) pentru Europa, Orientul apropiat şi Asia centrală), care le deleagă clienţilor lor (furnizori de servicii Internet sau organizaţii)[62]. În 3 februarie 2011, a fost alocată ultima adresă IPv4 către un *Regional Internet Registry*[63], ceea ce a impus trecerea la IPv6. Versiunea IPv6 a fost dezvoltată de Internet Engineering Task Force (IETF) şi este descrisă în documentul standard RFC 2460. IPv6 foloseşte numere de 128 de biţi şi are două părţi logice: un prefix de reţea de 64 biţi şi o parte adresă *host* de 64 biţi. Reprezentarea este de opt grupuri de 4 cifre hexazecimale, separate de caracterul ":" (folosirea protocolului fiind aprobată în 1999)[64].

Numele de domeniu pot fi înregistrate în spaţii cunoscute sub denumirea "nume generice de nivel de vârf" (*generic top-level domains - gTLDs*) sau în spaţii cunoscute sub denumirea "domenii de nivel de vârf cu cod de ţară" (*country code top-level domains - ccTLDs*)[65]. Există mai multe tipuri de TLD în sistemul numelor de domeniu:

---

[61] Valorile 0, 127 şi 255 sunt speciale, nu sunt utilizate pentru orice adrese IP – vezi în E. Nemeth şi colab., op. cit., p. 249-250.

[62] Vezi http://www.iana.org/numbers/.

[63] Vezi G. Huston, *A Rough Guide to Address Exhaustion*, The Internet Protocol Journal, Vol. 14, No. 1, March, 2011.

[64] Vezi Internet Corporation for Assigned Names and Numbers, *Abuse Issues and IP Addresses*, 2005. Vezi şi http://isoc.org/ipv6 şi http://www.iana.org/assignments/ipv6-address-space/ipv6 -address-space.xhtml.

[65] De regulă, numele de domenii sunt ierarhizate. La nivelul cel mai general al ierarhiei, se află numele ţărilor (spre exemplu, *.ro* (România), *.it* (Italia), *.ch* (Elveţia), *.fr* (Franţa)), sau tipul organizaţiei, cum ar fi, spre exemplu, *.gov* (pentru guvern). În continuare, urmează numele care se referă la o anumită entitate din acea ţară sau organizaţie, apoi numele care se referă la un anumit departament din instituţie şi în final numele care se referă la un anumit sistem informatic.

BCU CLUJ / CENTRAL UNIVERSITY LIBRARY

• Un TLD special *.arpa*, folosit pentru scopuri tehnice, administrat de ICANN în cooperare cu comunitatea tehnică Internet sub ghidarea Internet Architecture Board.

• TLD cu două litere au fost stabilite pentru peste 240 de ţări şi teritorii şi sunt referite drept “TLD cod de ţară” (*country-code TLD* sau *ccTLD*). Acestea sunt delegate unor manageri care le administrează în acord cu politici locale adaptate să satisfacă circumstanţele economice, culturale, lingvistice şi legale din ţara sau teritoriul respectiv.

• TLD cu trei sau mai multe litere, referite drept TLD generic sau *gTLD*, subdivizate în două categorii: sponsorizate şi nesponsorizate (*uTLD*). Un TLD sponsorizat este un TLD specializat care are un sponsor ce reprezintă o comunitare relativ reestrânsă, afectată de respectivul TLD, care are responsabilităţi privind formularea politicilor de folosire. Un TLD nesponsorizat este operat conform politicilor stabilite de comunitatea Internet, prin intermediul ICANN.

În anii `80, au fost create 7 gTLD: .com, .net, .org, .edu, .gov, .int şi .mil, primele trei fiind fără restricţii, celelalte având un scop limitat. În anii 2001-2002, au apărut 4 noi TLD nesponsorizate (.biz, .info, .name şi .pro) şi 3 noi TLD sponsorizate (.aero, .coop şi .museum). Ulterior au fost acceptate şi alte TLD, cum ar fi .asia, .cat, .jobs, .mobi, .name, .tel şi .travel.

Conform VeriSign[66], la sfârşitul anului 2013, existau peste 271 milioane înregistrări de nume de domeniu în Top Level Domains (TLDs), o creştere cu circa 18,5 milioane într-un an, iar în Country Code Top Level Domains (ccTLDs) existau 123,5 milioane nume. Domeniile .com şi .net au un număr combinat de peste 127.2 milioane nume. Cele mai mari TLDs sunt, în ordine, .com, .tk, .de, .net, .uk, .org, .cn, .info, .ru, .nl.

Cu toate avantajele prezentate de sistemul de nume de domeniu, bazat pe o clasificare logică, ce are la bază activitatea economică sau locaţia geografică, acesta a devenit unul dintre cele mai controversate aspecte în guvernarea Internetului, existând numeroase presiuni pentru liberalizarea sa. În iunie 2008, în cadrul celei de a 32-a adunări generale anuale, la care au participat circa 1500 de delegaţi din 70 de ţări, ICANN a aprobat liberalizarea sistemului numelor de domeniu[67]. Subsecvent, s-au înregistrate mii de aplicaţii pentru noile gTLDs, cum ar fi .music, .tech, .fashion, .youtube, .nike etc. (Google, spre exemplu, a aplicat pentru 98 de noi gTLDs[68])[69].

Printre cele mai întemeiate motive de opunere la un nume de domeniu se numără: încălcarea mărcilor de comerţ înregistrate, potenţiala confuzie[70] cu un

---

66 Vezi VeriSign, *The domain name industry brief*, Vol. 11, Iss. 1, April, 2014, disponibil la www.verisigninc.com/assets/domain-name-report-april2014.pdf.

67 https://www.icann.org/resources/board-material/resolutions-new-gtld-2014-05-14-en

68 Vezi https://domaintyper.com/new-gTLD/applicant/Google

69 Privind modalitatea de înreghistrare a noilor gTLS, vezi ICANN, *Applicant Guidebook*, http://newgtlds.icann.org/en/applicants/agb.

70 “Confuzia” este determinată pentru fiecare caz individual, în funcţie de un număr de criterii - vezi o discuţie detaliată în Lanning Bryer şi Matthew Asbell, *Combining trademarks in a jointly owned IP holding company*, The Trademark Reporter, 98, 834-872, 2008.

BCU IASI CENTRAL UNIVERSITY LIBRARY

nume de domeniu existent, reprezentarea eronată a unei comunităţi economice sau culturale sau atingerea moralităţii sau ordinii publice. Dacă doi sau mai mulţi aplicanţi doresc acelaşi nume de domeniu, ICANN solicită o înţelegere a părţilor[71], cu posibilitatea unei licitaţii în cazul în care nu se ajunge la o înţelegere între părţi. Persoanele fizice pot să întregistreze un nume de domeniu de vârf pe numele lor, în timp ce companiile pot înregistra nume de domeniu bazate pe proprietatea intelectuală deţinută.

[71] Vezi, spre exemplu, rezolvarea unor dispute privind domeniul *.la* (Laos v. Los Angeles) sau *.tv* (Tuvalu v. companii de televiziune).

BCU IASI/CENTRAL UNIVERSITY LIBRARY

2. AFACERI ELECTRONICE

2.1 Aspecte introductive

Globalizarea crescândă, micşorarea ciclului de viaţă al produselor, necesitatea unei eficienţe crescute şi pretenţiile din ce în ce mai mari ale clienţilor, au impus folosirea tehnologiilor moderne pentru desfăşurarea afacerilor. Natura deschisă a Internetului, caracterul său evolutiv, generativ[72] şi multifuncţional, permiţând un acces rapid, la scară globală şi la costuri din ce în ce mai reduse, au crescut potenţialul pentru aceasta nouă modalitate de afaceri, din ce în ce mai multe organizaţii migrând către activităţi desfăşurate electronic. Masiva infrastructură informatică schimbă modul în care oamenii sau firmele desfăşoară diverse activităţi, intern sau între ele, chiar modul în care funcţionează economia mondială[73] (putem vorbi, de fapt, despre competiţie între *lanţuri de furnizori*, mai mult decât de competiţie între firme individuale).

În cadrul comerţului electronic (*e-commerce*), sunt folosite numeroase aplicaţii informatice (spre exemplu, *relationship-marketing*, *customer management*, e-*procurement* etc.), pentru interacţiuni cu clienţi sau furnizori, pentru integrarea activităţilor, pentru o eficienţă crescută privind colectarea plăţilor[74] şi pentru a crea noi posibilităţi de export sau surse de venit. Comerţul electronic reprezintă o parte importantă a comerţului internaţional, vânzările globale *business-to-consumer* (B2C) fiind estimate la 1,5 trilioane dolari în 2014[75]. Creşterea ca procent din vânzările globale este, de asemenea, impresionantă: în SUA, spre exemplu, în primul trimestru 2014, comerţul electronic a crescut cu 15% faţă de primul trimestru 2013, în timp ce, în aceeaşi perioadă, vânzările totale au crescut doar cu 2.4% [76].

Agenda Digitală pentru Europa stabileşte obiectivul ca 50% din populaţie să cumpere online până în anul 2015. Avantajele comerţului electronic sunt multiple, totuşi, mijloacele electronice reprezintă doar un vector, principiile şi cadrul legal pentru desfăşurarea afacerilor rămânând valabile.

---

72 Vezi J. L. Zittrain, *The Generative Internet*, Harvard Law Review, 119, 1974-2040, 2006.

73 Vezi statistici în U.S. Census Bureau (http://www.census.gov/mrts/www/ecomm.html); comScore, conform căruia comerţul electronic va atinge $170 miliarde în 2006, August 2, 2006, la http://www.comscore.com/press/release.asp?press=959.

74 D. B. Humphrey & R. Hunt, *Cost Savings from Check 21 Electronic Payment Legislation*, Journal of Money, Credit and Banking, 45, 1415, 2013.

75 eMarketer, *Global B2C Ecommerce Sales to Hit $1.5 Trillion This Year Driven by Growth in Emerging Markets*, 2014, disponibil la locaţia http://www.emarketer.com/Article/Global-B2C-Ecommerce-Sales-Hit-15-Trillion-This-Year-Driven-by-Growth-Emerging-Markets/1010575.

76 United States Census Bureau, *Quarterly retail e-commerce sales 1ST quarter*, 2014.

BCU IASI/CENTRAL UNIVERSITY LIBRARY

2.2 Tipuri de afaceri

Afacerile electronice au devenit un fenomen global. Există mai multe tipuri de afaceri internaţionale: *comerţ, licenţierea de tehnologie* sau *drepturi de proprietate intelectuală* şi *investiţii directe*.

Comerţ

Într-un mediu de afaceri, părţile intră într-o mare varietate de tipuri de tranzacţii: contracte privind vânzarea-cumpărarea de bunuri, de închiriere, de împrumut, de achiziţionare de instrumente negociabile, de licenţiere, de asignare de drepturi sau titluri, de asigurări, proxy etc., toate acestea putând fi realizate foarte eficient în cyberspaţiu[77]. Conform Directivei EU 98/48/EC, "comerţ electronic" este orice serviciu furnizat pentru o remuneraţie, de la distanţă, prin mijloace electronice, la solicitarea individuală a recipientului serviciului. Conform Organizaţiei Mondiale a Comerţului, "comerţul electronic" este definit ca fiind producţia, distribuţia, marketingul, vânzarea sau furnizarea de bunuri şi servicii prin mijloace electronice[78].

Principalele tipuri de comerţul electronic sunt B2C (*Business to Consumer*), C2C (*Consumer to Consumer*), B2B (*Business to Business*), G2B (*Government to Business*) şi B2G (*Business to Government*). Comerţul electronic acoperă schimburi de informaţii şi tranzacţii privind produse, echipamente sau bunuri de consum curent şi servicii (incluzând servicii de informare, financiare, juridice etc.). Comerţul electronic include două tipuri de activităţi: *comerţ electronic indirect* (comandarea electronică de bunuri tangibile, care sunt expediate fizic folosind canale tradiţionale, cum ar fi serviciile poştale) şi *comerţ electronic direct* (comanda, plata şi livrarea electronică de bunuri intangibile, cum ar fi programe informatice sau filme în format digital).

Licenţierea drepturi de proprietate intelectuală sau de tehnologie

Licenţierea drepturilor de proprietate intelectuală se referă la dreptul legal de a folosi brevete, mărci de comerţ şi/sau drepturi de autor, pentru o perioadă specificată de timp, în schimbul unei sume de bani. Licenţierea de tehnologie se referă la transferul de *know-how* sau de tehnologii, între firme sau guverne. Franciza este o formă de licenţiere în care beneficiarul poate folosi o marcă comercială, know-how în administrarea sau managementul unei firme sau secrete comerciale, de obicei fiind folosită în activităţi de tip *en detail*.

---

[77] Vezi T. J. Smedinghoff, *The Legal Requirements for creating secure and enforceable electronic transactions*, 2002.

[78] Vezi Declaraţia WTO asupra comerţului electronic din 25 septembrie 1998.

BCU IASI CENTRAL UNIVERSITY LIBRARY

Investiții directe

Investiţiile directe pot lua diverse forme: finanţarea unei noi firme ca subsidiară, formarea unui *joint venture* cu o companie existentă sau achiziţionarea unei firme.

2.3 Modele de afaceri electronice

Un "model de afaceri" este *metoda* prin care o entitate generează venituri. Există o mulţime de modele de afaceri electronice, noi modele apărând constant[79]. Fiecare model de afaceri este caracterizat de o combinaţie de elemente, printre acestea numărându-se tipul de tehnologie de transport (*downloading* sau *streaming*); tipul de proprietate intelectuală folosit pentru distribuţie (deschis sau protejat); tipul de sistem de management digital al drepturilor folosit; structura de preţ folosită; nivelul de interactivitate etc.

Modelele de afaceri electronice pot fi împărţite în două categorii mari: *Modele transplantate din lumea reală* (spre exemplu, folosirea unei locaţii Web pentru a vinde bunuri fizice) şi *Modele native Internet* (modele specifice mediului electronic). O taxonomie a modelelor de afaceri electronice este propusă de Hodge şi Cagle[80]. Clasificări cunoscute ale modelelor de afaceri electronice sunt cele propuse de P. Bambury[81] (*modele transplantate din lumea reală*: comadă poştală, reclame, abonament, testare gratuită, direct marketing etc.; *modele native Internet*: freeware, bibliotecă, schimb informaţional, furnizare acces, găzduire web sau alte servicii Internet şi produse digitale); T. Eisenmann[82] (vânzări cu amănuntul, portaluri online, furnizori de access Internet, furnizori de conţinut digital, furnizori de aplicaţii, brokeri online etc.); M. Rappa[83] (comerciant, reclamă, abonament, comunitare, manufactură, infomediar etc.); sau P. Timmers[84] (*e-shop*, *e-auction*, *e-mall*, *e-procurement*, comunităţi virtuale, integratori de furnizori, platforme de colaborare, broker de informaţii etc.).

---

79 Vezi Gandolfo Dominici, *E-Business Model: A Content Based Taxonomy of Literature*, International Journal of Management and Administrative Sciences, 1(7), April, 10-20, 2012; Christoph Zott, Raphael Amit şi Lorenzo Massa, *The Business Model: Recent Developments and Future Research*, Journal of Management, 37 (4), 1019-1042, 2011; J. Gordijn, J. Akkermans şi J. Van Vliet, *Designing and Evaluating E-Business Models*, IEEE Intelligent Systems, 16 (4), 11-17, 2001; K. Vassilopoulou şi colab., *E-Business models: A Proposed Framework*, 2002.

80 Vezi G. Hodge şi C. Cagle, *Business-to-Business E-Business models: Classification and textile industry implications*, AUTEX Research Journal, Vol. 4 (4), 2004.

81 Vezi P. Bambury, *A Taxonomy of Internet Commerce*, First Monday, 3 (10), 1998.

82 Vezi T. Eisenmann, *Internet Business Models: Text and Cases*, McGraw-Hill Irwin, 2002.

83 Vezi M. Rappa, *Business Models on the Web*, 2001.

84 Vezi P. Timmers, *Business Models for Electronic Markets*, Electronic Markets, 8 (2), 1998.

BOURGAS CENTRAL UNIVERSITY LIBRARY

2.4 Cadrul legal privind tranzacţiile electronice

Pentru a face afacerile electronice viabile din punct de vedere legal, comunicaţiile sau tranzacţiile care au loc, precum şi înregistrările acestora, trebuie să poată răspunde la următoarele întrebări[85]:

- Tranzaţiile în cauză sunt autorizate în formă electronică?
- Procesul electronic va rezulta într-un contract cu valoare legală?
- Au fost furnizate toate informaţiile cerute de legile privind tranzacţiile electronice?
- Înregistrările tranzacţiilor sunt accesibile părţilor?
- A fost folosită o semnătură electronică validă?
- Tranzacţia este de încredere?
- Înregistrările electronice sunt păstrate?

Tranzacţiile electronice sunt guvernate de numeroase reglementări şi cerinţe legale[86]:

SUA

- The Uniform Computer Information Transactions Act (UCITA, 2002);
- The Uniform Electronic Transactions Act (UETA, 1999); şi
- Electronic Signatures in Global and National Commerce Act (Millennium Digital Commerce Act sau E-SIGN), Pub. L. No. 106-229, 114 Stat. 464 (2000) - 15 U.S.C. § 7001 et seq.

UE

- Directiva privind semnăturile electronice (1999/93/EC) şi COM/2008/0798 final (Plan de acţiune privind semnăturile electronice şi identificarea electronică pentru facilitarea furnizării de servicii publice transfrontaliere pe piaţa unică);
- Directive privind protecţia datelor (95/46/EC, 97/66/EC şi 2002/58/EC);
- Directiva 2011/83/UE a Parlamentului European şi a Consiliului din 25 octombrie 2011 privind drepturile consumatorilor, de modificare a Directivei 93/13/CEE a Consiliului şi a Directivei 1999/44/CE a Parlamentului European şi a Consiliului şi de abrogare a Directivei 85/577/CEE a Consiliului şi a Directivei 97/7/CE a Parlamentului European şi a Consiliului (*Directive on Consumer Rights*). Conform Directivei 2011/83/UE, "contract la distanţă" înseamnă orice "contract

[85] Conform T. J. Smedinghoff, *Seven Key Legal Requirements for Creating Enforceable Electronic Transactions*, 2005; Directiva 2000/31/EC a Parlamentului European asupra anumitor aspecte legale ale serviciilor societăţii informationale, în particular comerţul electronic.

[86] Vezi, spre exemplu, R. L. Trope şi G. E. Upchurch, *Checkpoints in Cyberspace: Best Practices to Avert Liability in Cross-Border Transactions*, American Bar Association, 2005; M. J. Radin şi D. Appelman, *Doing Business in the Digital Era: Some Basic Issues*, 1999; T. Cox, *Information and the Internet: Understanding the Emerging Legal Framework for Contract and Copyright Law and Problems with International Enforcement*, 11 Transnational Law, 23, 1998.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

încheiat între comerciant și consumator în cadrul unui sistem de vânzări sau de prestare de servicii la distanță organizat, fără prezența fizică simultană a comerciantului și a consumatorului, cu utilizarea exclusivă a unuia sau a mai multor mijloace de comunicare la distanță, până la și inclusiv în momentul în care este încheiat contractul"[87].

- Directiva privind comerțul electronic (2000/31/EC - *Certain Legal Aspects of Information Society Services, in particular Electronic Commerce in the Internal Market*)[88], care cuprinde aspecte importante, cum ar fi:
  - Regula țării de origine pentru stabilirea legii aplicabile;
  - Transparența termenilor și condițiilor contractuale;
  - Încheierea contractelor: stipulează cerințe extensive privind informația necesară înainte de încheierea contractelor și o procedură în 3 pași pentru formarea acestora;
  - Protecția datelor;
  - Protecția consumatorilor;
  - Responsabilitatea pentru conținut.

Legislația europeană și cea din SUA sunt similare, totuși legile americane sunt mai largi în ceea ce privește domeniul acoperit. Astfel, UETA acoperă toate tipurile de contracte, nu numai contractele electronice, iar UCITA acoperă toate tipurile de informații privind contractele. În contrast, Directivele UE se ocupă numai cu contracte privind consumatorii, exceptând tranzacțiile B2B[89].

Cadrul legal internațional

- UNCITRAL Model Law on Electronic Commerce (General Assembly Resolution 51/162 din 16 decembrie 1996);
- UNCITRAL Model Law on Electronic Signatures (2001);
- The United Nations Convention on the Use of Electronic Communications in International Contracts (2005)[90].

Convenția on the *Use of Electronic Communications in International Contracts*, propusă de UNCITRAL, adoptată de *General Assembly* în 23 noiembrie 2005 prin rezoluția 60/21 și deschisă pentru semnare din 16 ianuarie 2006 până în 16 ianuarie 2008, propune soluții practice la problemele legate de folosirea mijloacelor electronice în contracte internaționale și se aplică la folosirea

---

87 Conform Directivei 2011/83/UE, "un contract negociat în spațiile comerciale ale comerciantului și în final încheiat prin intermediul mijloacelor de comunicare la distanță nu ar trebui considerat un contract la distanță". Vezi descrierea principalelor modificări pentru consumatori în European Commission, MEMO/11/450, 23/06/2011.

88 Comisia Europeană, după realizarea unei consultări publice, a decis că nu este necesară actualizarea acestei Directive și a adoptat *e-Commerce Communication* (2012) - vezi http://ec.europa.eu/digital-agenda/en/pillar-i-digital-single-market/action-9-updating-ecommerce-directive

89 Privind formarea contractelor, vezi Sylvia Mercado Kierkegaard, *E-Contract Formation: U.S. and EU Perspectives*, 3 Shidler Journal of Law, Commerce and Technology, 12, 2007.

90 În anul 2005, Comisia Europeană a solicitat un mandat de la Consiliul Europei pentru a negocia cu UNCITRAL asupra Convenției pentru a asigura compatibilitatea cu Directiva 2000/31/EC.

comunicaţiilor electronice în conexiune cu formarea şi executarea unui contract între părţi ale căror locuri de desfăşurare a afacerilor sunt plasate în state diferite. Această Convenţie nu se aplică la comunicaţiile electronice legate de contracte încheiate pentru scopuri personale sau familiale, tranzacţii reglementate, tranzacţii cu devize internaţionale, tranzacţii inter-bancare de plăţi sau obligaţiuni, răscumpărarea de bunuri sau instrumente financiare păstrate de un intermediar.

Datorită naturii lor, comunicaţiile electronice pot traversa sau exista în jurisdicţii diferite. Un aspect important în cadrul afacerilor electronice priveşte *alegerea jurisdicţiei* în conflictele internaţionale[91]. Aspectele privind alegerea jurisdicţiei sunt delicate şi au fost analizate în numeroase articole[92].

Astfel, o tranzacţie poate implica mai multe jurisdicţii. Spre exemplu, o persoană din statul 1 poate iniţia o tranzacţie printr-un calculator aflat în statul 2, tranzacţia fiind recepţionată de o persoană din statul 3 care are acces Internet printr-un server localizat în statul 4 şi care va rezolvată printr-o expediere de bunuri fizice la o locaţie situată în statul 5[93]. În SUA, spre exemplu, cele mai utilizate metode pentru rezolvarea disputelor privind jurisdicţia sunt *lex loci delicti* (care se referă la locul unde s-a petrecut ultimul eveniment necesar pentru a face o parte responsabilă pentru o acţiune) şi "cea mai semnificativă relaţie".

Firmele care oferă bunuri sau servicii prin mijloace electronice trebuie să definească cu atenţie locul unde eventualele dispute vor fi soluţionate (spre exemplu, prin folosirea de *Terms of Service*). În cazul în care părţile implicate optează pentru arbitraj, trebuie menţionat organismul care va face acest lucru [spre exemplu, Camera Internaţională de Comerţ, Comisia Naţiunilor Unite pentru Dreltup Comerţului Internaţional (UNCITRAL), American Arbitration Association, Centrul Internaţional pentru Rezolvarea Disputelor de Investiţii etc.].

Conform art. 4 (h) al *Convention on the Use of Electronic Communications in International Contracts*, "loc de desfăşurare al afacerilor" (*place of business*) este orice loc unde o parte are un stabiliment non-tranzitoriu pentru a desfăşura o activitate economică, alta decât furnizarea temporară de bunuri sau servicii de la o locaţie. Conform Convenţiei, "loc de desfăşurare a afacerilor" este prezumat a fi locaţia indicată de parte, dacă o altă parte nu demonstrează că partea făcând

---

91 Conflictele internaţionale sunt reglementate folosind legi de Drept Internaţional Privat şi Convenţii multilaterale (spre exemplu, The International Convention for the Sale of Goods, The Recognition and Enforcement of Foreign Arbitral etc.). Vezi şi The Convention on the Law Applicable to Contractual Obligations (80/934/EEC), precum şi The Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters şi The Lugano Convention on Jurisdiction and the Enforcement in Civil and Commercial Matters.

92 Vezi, spre exemplu, E. Katsh şi colab., *E-Commerce, E-Disputes, and E-Dispute Resolution: In the Shadow of "Ebay Law"*, 15 Ohio State Journal On Dispute Resolution 705, 2000; J. K. Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 Tulane Law Review, 1177, 1998; D. Johnson şi D. Post, *Law And Borders - The Rise of Law in Cyberspace*, 48 Stanford Law Review, 1367 şi urm., 1996.

93 Vezi în J. Rothchild, *Protecting the Digital Consumer: The Limits of Cyberspace Utopianism*, Indiana Law Journal, Summer, 893, 1999; vezi, de asemenea, J. L. Goldsmith, *Against Cyberanarchy*, University of Chicago Law Review, Fall, 1199, 1998; R. M. Frieden, *Universal service: When technologies converge and regulatory models diverge*, Harvard Journal of Law & Technology, Vol. 13, No. 3, Summer, 2000.

indicația nu are un loc de desfășurare a afacerilor la acea locație. Conform art. 6, dacă o parte nu a indicat un "loc de desfășurare a afacerilor" și are mai mult de un astfel de loc, "locul" va fi cel care are cea mai apropiată legătură cu contractul relevant, luând în considerare circumstanțele cunoscute părților la momentul încheierii contractului). Dacă o persoană fizică nu are un "loc de desfășurare a afacerilor", referința va fi făcută la reședența respectivei persoane.

O locația nu va fi considerată "loc de desfășurare a afacerilor" doar pentru că acolo se află echipament sau tehnologii asociate unui sistem informatic folosit pentru a încheia contractul sau unde un sistem informatic poate fi accesat de alte părți. Simplul fapt că o parte folosește un nume de domeniu sau adresă de poștă electronică asociată unei țări nu crează prezumpția că acela este locul de desfășurare a afacerilor.

Conform art. 8, validitatea sau puterea legală a unei comunicații sau a unui contract nu va putea fi disputată doar pe motivul că este în forma unei comunicații electronice. Valabilitatea sau puterea legală a unui contract, format prin interacțiuned dintre un sistem automat de mesaje și o persoană fizică, sau prin interacțiunea dintre sisteme automate, nu va fi negată pe simplul motiv că nici o persoană fizică nu a revăzut sau intervenit în fiecare din acțiunile individuale realizate de sisteme automate sau contractul rezultat (confom art. 12).

Conform art. 9, acolo unde legea solicită ca o comunicație sau contract să fie în scris, sau precizează consecințe pentru absența scrieri, acea cerință este satisfăcută de o comunicare electronică, dacă informația conținută este accesibilă pentru a fi folosită pentru referință subsecventă. Acolo unde legea solicită ca o comunicare sau un contract să fie semnat de părți, sau precizează consecințe pentru absența unei semnături, acea cerință este satisfăcută în relație cu o comunicare electronică dacă:

- O metodă este folosită pentru identificarea părții și a intenției acelei părți cu privire la informația conținută în comunicarea electronică și
- Metoda folosită este fie:
  - Fiabil adecvată pentru scopul în care comunicarea este generată sau comunicată, în lumina tuturor circumstanțelor, incluzând orice înțelegere relevantă, sau
  - Dovedită a fi satisfăcut funcțiile descrise în subparagraful de mai sus, în sine sau cu evidențe suplimentare.

Acolo unde legea solicită ca o comunicare sau un contract să fie făcut disponibil sau păstrat în forma sa originală, sau prevede consecințe în lipsa unui original, acea cerință este satisfăcută în relație cu o comunicare electronică dacă:

- Există o asigurare fiabilă privind integritatea informației conținută din momentul generării în forma sa finală, ca o comunicare electronică sau altfel [4 (a)] și
- Acolo unde este necesar ca informația conținută să fie făcută disponibilă, ea poate fi afișată pentru persoana pentru care este făcută disponibilă [4 (b)].

BCU IASI / CENTRAL UNIVERSITY LIBRARY

Pentru scopul paragrafului de mai sus [4 (a)], criteriul pentru evaluarea integrității va privi rămânerea completă și nealterată a informației, separat de adăugarea de susțineri (*endorsement*) și orice modificări care apar în cursul normal al comunicației, stocării și afișări. Standardul de fiabilitate solicitat va fi evaluat în lumina scopului pentru care informația a fost generată și în lumina tuturor circumstanțelor relevante.

Momentul și locul comunicațiilor electronice sunt foarte importante în cadrul afacerilor electronice. Conform art. 10, momentul transmiterii unei comunicații electronice este momentul când părăsește un sistem informatic aflat sub controlul originatorului sau al părții care a transmis în numele originatorului său. Dacă respectiva comunicare electronică nu a părăsit un sistem informatic aflat sub controlul originatorului sau al părții care l-a transmis în numele originatorului, "momentul" este considerat când comunicarea electronică este recepționată.

Momentul recepționării unei comunicații electronice este momentul în care aceasta devine disponibilă adresantului la adresa electronică desemnată de acesta. Momentul recepționării unei comunicații electronice la o altă adresă electronică a adresantului este momentul când devine capabil să o acceseze la acea adresă și este conștient că acolo a fost transmisă comunicarea electronică. O comunicare electronică se prezumă a fi disponbibilă pentru adresant în momentul în care ajunge la adresa sa electronică.

România

În România, Legea nr. 365 din 7 iunie 2002 stabilește cadrul legal pentru desfășurarea comerțului electronic. Contractele încheiate la distanță[94] sau prin mijloace electronice produc toate efectele pe care legea le recunoaște în cazul contractelor clasice, dacă sunt respectate condițiile legale pentru valabilitatea acestora: condiții de fond (art. 948 din Codul Civil, privind capacitatea și consimțământul părților, obiectul și cauza contractului) și condiții de formă.

Astfel, Legea nr. 365/2002 (art. 7) stipulează următoarele: contractele încheiate prin mijloace electronice produc toate efectele pe care legea le recunoaște contractelor, atunci când sunt întrunite condițiile legale pentru validitatea acestora. Pentru validitatea contractelor încheiate prin mijloace electronice nu este necesar consimțământul prealabil al părților asupra utilizării de mijloace electronice. Proba încheierii contractelor prin mijloace electronice și a obligațiilor care rezultă din aceste contracte este supusă dispozițiilor dreptului comun în materie de probă și prevederilor Legii nr. 455/2001 (privind semnătura electronică).

Conform art. 8 al Legii nr. 365/2002, furnizorul de servicii este obligat să pună la dispoziție destinatarului, înainte ca destinatarul să trimită oferta de a contracta sau acceptarea ofertei ferme de a contracta făcute de furnizorul de

94 Directiva europeană 97/7/CE din 20 mai 1997 folosește termenul de "contract la distanță", pe care-l definește ca "orice contract privind bunuri sau servicii încheiat între un furnizor și un consumator în cadrul unui sistem de vânzări sau de prezentări la distanță organizat de către furnizor, care, pentru acest contract, utilizează exclusiv una sau mai multe technici de comunicare la distanță".

servicii, cel puţin următoarele informaţii care trebuie să fie exprimate în mod clar, neechivoc şi într-un limbaj accesibil:

- Etapele tehnice care trebuie urmate pentru a încheia contractul;
- Dacă contractul, o dată încheiat, este stocat sau nu de către furnizorul de servicii şi dacă este accesibil sau nu;
- Mijloacele tehnice pe care furnizorul de servicii le pune la dispoziţie destinatarului pentru identificarea şi corectarea erorilor survenite cu ocazia introducerii datelor;
- Limba în care se poate încheia contractul;
- Codurile de conduită relevante la care furnizorul de servicii subscrie, precum şi informaţii despre modul în care aceste coduri pot fi consultate prin mijloace electronice;
- Orice alte condiţii impuse prin dispoziţiile legale în vigoare.

Încheierea contractului prin mijloace electronice

Conform Legii nr. 365/2002 (art. 9), dacă părţile nu au convenit altfel, contractul se consideră încheiat în momentul în care acceptarea ofertei de a contracta a ajuns la cunoştinţa ofertantului. Contractul care, prin natura sa ori la cererea beneficiarului, impune o executare imediată a prestaţiei caracteristice, se consideră încheiat în momentul în care debitorul acesteia a început executarea, în afară de cazul în care ofertantul a cerut ca în prealabil să i se comunice acceptarea.

Conform alin. 3 al art. 9, în cazul în care destinatarul trimite prin mijloace electronice oferta de a contracta sau acceptarea ofertei ferme de a contracta făcute de furnizorul de servicii, furnizorul de servicii are obligaţia de a confirma primirea ofertei sau, după caz, a acceptării acesteia, în unul dintre următoarele moduri:

- Trimiterea unei dovezi de primire prin poşta electronică sau printr-un alt mijloc de comunicare individuală echivalent, la adresa indicată de către destinatar, în termen de 24 de ore de la primirea ofertei sau acceptării;
- Confirmarea primirii ofertei sau a acceptării ofertei, printr-un mijloc echivalent celui utilizat pentru trimiterea ofertei sau a acceptării ofertei, de îndată ce oferta sau acceptarea a fost primită de furnizorul de servicii, cu condiţia ca această confirmare să poată fi stocată şi reprodusă de către destinatar.

Oferta sau acceptarea ofertei, precum şi confirmarea primirii ofertei sau a acceptării ofertei, efectuate în unul dintre modurile prevăzute la alin. 3, se consideră primite atunci când părţile cărora le sunt adresate pot să le acceseze. Prevederile alin. 3 nu se aplică în privinţa contractelor încheiate exclusiv prin poştă electronică sau prin alte mijloace de comunicare individuală echivalente.

Păstrarea sau prezentarea informaţiei

Conform Legii nr. 365/2002 (art. 10), acolo unde legea impune ca informaţia să fie prezentată sau păstrată în forma sa originală, această cerinţă este îndeplinită dacă sunt întrunite în mod cumulativ următoarele condiţii:

BUCHAREST UNIVERSITY LIBRARY

- Există garanția integrității informației, asigurată prin respectarea standardelor naționale în domeniu, din momentul în care a fost generată;
- Mesajul este semnat utilizându-se semnătura electronică extinsă a emitentului;
- Informația poate fi imediat furnizată și prezentată la cerere.

Destinatarul comerciant acționează pe riscul propriu, dacă a știut, sau ar fi trebuit să știe, în concordanță cu practicile comerciale curente sau ca urmare a folosirii procedurilor convenite expres cu emitentul, că informația conținută într-un mesaj electronic a fost alterată în timpul transmiterii sau prelucrării sale.

2.5 Tipuri de contracte electronice

Afacerile electronice au determinat apariția de noi tipuri de contracte, acestea fiind încheiate între o persoană și un calculator sau între două calculatoare, administrate de oameni de la distanță. Directiva 2000/31/EC prevede, în Art. 9, obligația statelor membre să asigure transpunerea prevederilor privind contractele electronice în legislația națională. Clasificarea contractele electronice se poate face după mai multe criterii: *modul de încheiere*: contracte reactive (care implică executarea unui click asupra unui buton sau pictogramă) sau interactive (care implică acceptarea tacită a unor termeni sau clauze); *modul de executare*: contracte directe (transmiterea de bunuri imateriale sau furnizarea de servicii) sau indirecte; *momentul execuției*: imediate sau în curs de executare; după *subiecții* contractului (firme, guverne sau persoane fizice); după *metoda de plată* acceptată etc.

Prof. M. J. Radin[95] distinge două modele de contracte electronice: **Modelul "contract-consimțământ"** (*Contract-as-consent*, care implică consimțământul a două persoane) și **Modelul "contract-produs"** (*Contract-as-product*, ai cărui termeni sunt parte a produsului, nu o parte conceptuală separată). Privind modul de formare a contractelor electronice, Prof. M. J. Radin distinge trei metode: "click-wrap", "machine-made" și "viral"[96].

Contractul de tip "Click": Multe site-uri web conțin termeni ai serviciului (*Terms of Service*) și condiții de folosire (*Conditions of Use*)[97]. Contractele de tip "click" sunt de tip interactiv și solicită un răspuns din partea consumatorului, pentru a intra în vigoare. Contractele de tip "click" necesită îndeplinirea următoarelor condiții pentru a avea putere juridică: informare asupra posibilității de apariție a unor termeni contractuali adiționali după termenii inițiali, dreptul de a returna produsul la costul inițial, compensarea consumatorului pentru daune cauzate de produsul achiziționat (spre exemplu, în cazul instalării unui program informatic)[98].

---

95 Vezi M. J. Radin, *Humans, Computers, and Binding Commitment*, Indiana Law Journal, Vol. 75, 1999.

96 *Id.*, p. 1128.

97 Pentru detalii vezi *id.*, p. 1129-1130.

98 Pentru detalii, vezi R. Cormier Anderson, *Enforcement of Contractual Terms in Clickwrap Agreements*, Shidler Journal of Law, Commerce, and Technology, 3, 11, 2007.

Contracte realizate de calculator: Contractele din această categorie pot fi clasificate ca implicând calculatoarele ca "agenţi electronici" sau ca "mijloace electronice" de aplicare sau respectare a unor reguli presetate[99]. În prima categorie, două calculatoare (nu între două persoane umane sau un om şi un calculator) "negociază" între ele pentru a ajunge la o înţelegere[100]. În cea de a doua categorie, cunoscută ca "sisteme de management digital al drepturilor" [*Digital Rights Management Systems* (DRM)] sau "sisteme de încredere" (*trusted systems*), programe informatice asigură respectarea termenilor prestabiliţi pentru un transfer de conţinut digital[101].

Contractul de tip "viral": Contractele de acest tip urmăresc asigurarea unor reguli sau obligaţiuni asociate unui obiect digital (spre exemplu, nealterarea sau imposibilitatea înlocuirii unor elemente, cum ar fi numele producătorului etc.), reprezentând o instanţiere a modelului de *contract-produs*[102] (un exemplu este oferit de programele informatice de tip *open source*[103]).

Conform altor autori[104], contractele electronice pot fi de tip "click" (*click-through* - acestea impun executarea unui click pe o pictogramă, buton sau *check box*[105], ca manifestare a acceptării termenilor contractului), respectiv de tip "browse" (*browse-wrap* - acest tip de contracte bazându-se pe termeni sau condiţii afişate pe pagini web, de regulă accesate prin legături *hypertext*, design-ul site-ului având semnificaţie contractuală[106], acceptarea fiind bazată pe "folosirea" unui site web, nesolicitând o acţiune afirmativă[107]).

2.6 Securitate informatică

Conform Directivei COM(2013) 48, "securitate" înseamnă "capacitatea unei reţele sau a unui sistem informatic de a rezista, la un nivel de încredere dat, unei acţiuni accidentale sau răuvoitoare care compromite disponibilitatea, autenticitatea, integritatea sau confidenţialitatea datelor stocate sau transmise ori a serviciilor conexe oferite de reţeaua sau de sistemul informatic respectiv sau accesibile prin intermediul acestora".

---

[99] *Id.*, p. 1130.
[100] *Id.*, p. 1130.
[101] *Id.*, p. 1131.
[102] *Id.*, p. 1132.
[103] *Id.*, p. 1132.
[104] Vezi R. J. Mann şi T. Siebeneicher, *Just one click: The reality of Internet retail contracting*, Columbia Law Review, Vol. 108, 984-1012, 2008; Christina L. Kunz şi colab., *Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements*, The Business Lawyer, Vol. 59, No. 1, November, 279-312, 2003; Ian Rambarran şi Robert Hunt, *Are Browse-Wrap Agreements All They Are Wrapped Up To Be?*, 9 Tulane Journal of Technology and Intellectual Property 173, 2007.
[105] Vezi Scherillo v. Dun & Bradstreet, Inc., 684 F. Supp. 2d 313 (E.D. N.Y. 2010).
[106] Vezi Woodrow Hartzog, *Website Design as Contract*, American University Law Review, 60 (6), 1635-1671, 2011.
[107] Vezi, spre exemplu, Hines v. Overstock.com, Inc., 668 F. Supp. 2d 362 (E.D. N.Y. 2009).

Autenticitatea priveşte sursa unei comunicaţii. Autenticitatea este atât o cerinţă de afaceri practică, cât şi una legală. Partea care crează contracte, licenţiază informaţii sau proprietate intelectuală, sau face plăţi electronice, trebuie să aibă siguranţa în ceea ce priveste autenticitatea comunicaţiilor recepţionate.

Pe de altă parte, dacă o entitate nu verifică identitatea sursei solicitării, ea poate fi făcută responsabilă pentru eventualele pierderi. Stabilirea autenticităţii unei tranzacţii electronice este importantă şi în cazul disputelor. Acestea solicită un mecanism pentru stabilirea autenticităţii şi pentru păstrarea unei înregistrări corecte a comunicaţiei şi a mijloacelor de autentificare, în cazul în care autentificarea este disputată.

Nonrepudierea se referă la abilitatea de a nu permite transmiţătorului să nege că ar fi iniţiat o tranzacţie sau că ar fi transmis o comunicaţie, dacă într-adevăr a iniţiat-o sau transmis-o, sau să pretindă că nu avem de a face cu un conţinutul real al tranzacţiei sau comunicaţiei. Nonrepudierea este esenţială în unele situaţii (spre exemplu, un broker care acceptă ordine de cumpărare/vânzare pe Internet nu va dori să aibă dispute repudiabile cu clienţi care plasează ordine şi după aceea, în funcţie de mişcările pieţei (sus/jos), confirmă sau contestă ordinul). Nonrepudierea devine o cerinţă legală când una dintre părţi dispută un contract.

Cerinţele de securitate ale sistemelor informatice, foarte numeroase şi complexe, au la bază numeroase aspecte operaţionale, economice, tehnice, politice, legale, societale şi umane:

- *Aspecte legale* – Legi şi reglementări ce trebuie luate în considerare de manageri şi incorporate în politicile de securitate.
- *Aspecte organizaţionale şi administrative* – Aspectele organizaţionale critice includ: dedicaţia managerilor, proceduri privind aplicarea, monitorizarea, auditul politicilor de securitate etc.
- *Aspecte societale* – Organizaţiile trebuie să satisfacă nevoi societale prin furnizarea unui nivel adecvat de securitate a sistemelor informatice pentru entităţi externe (spre exemplu, prin furnizarea unui acces adecvat la respectivele sisteme).
- *Standarde* – Organizaţiile trebuie să adere la standardele existente, ceea ce influenţează politicile de securitate a sistemelor de informaţii.
- *Aspecte privind sănătatea şi integritatea corporală a angajaţilor.*

Cerinţe legale privind securitatea datelor informatice

Lupta împotriva criminalităţii informatice reprezintă un element fundamental din perspectiva securităţii informatice[108]. La nivelul UE, Directiva 2009/136/CE prevede obligaţia asigurării unui nivel adecvat de protecţie a confidenţialităţii şi de securitate a datelor cu caracter personal transmise sau prelucrate în legătură cu utilizarea reţelelor de comunicaţii electronice pe piaţa internă. Directiva 2009/140/CE a Parlamentului European şi a Consiliului din 25 noiembrie 2009, pe de altă parte, impune luarea de măsuri tehnice şi

[108] Vezi Comunicarea Comisiei Europene, *Către o politică generală de luptă împotriva criminalităţii cibernetice*, COM(2007) 267 final; vezi şi D. B. Hollis, *An e-SOS for Cyberspace*, Harvard International Law Journal, 52 (2), Summer, 2011.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

organizatorice corespunzătoare pentru a gestiona în mod corespunzător riscurile privind securitatea rețelelor și serviciilor.

Directiva 2006/24/CE a Parlamentului European și a Consiliului prevede supunerea datelor informatice unor măsuri tehnice și organizaționale adecvate, pentru a fi protejate împotriva distrugerii accidentale sau ilegale, pierderii accidentale sau modificării, depozitării, prelucrării, accesării sau divulgării neautorizate sau ilicite. Datele se supun măsurilor tehnice și organizaționale adecvate pentru a se asigura că accesarea acestora poate fi făcută numai de către personal special autorizat și datele sunt distruse la finalul perioadei de păstrare, cu excepția celor care au fost accesate și reținute. Directiva 2002/21/EC solicită, de asemenea, măsuri adecvate pentru asigurarea integrității și securității datelor.

Convenția Europeană din 2001 și Decizia-cadru 2005/222/JAI a Consiliului din 24 februarie 2005 privind atacurile împotriva sistemelor informatice și Propunerea de Directivă a Parlamentului European și a Consiliului privind atacurile împotriva sistemelor informatice și de abrogare a Deciziei-cadru 2005/222/JAI a Consiliului [SEC(2010) 1122 final, SEC(2010) 1123 final] stipulează răspunderea persoanelor juridice. Astfel, o persoană juridică poată fi trasă la răspundere atunci când lipsa de supraveghere sau control imputabilă unei persoane a făcut posibilă săvârșirea unor infracțiuni informatice. Adițional, Regulamentul (CE) nr. 45/2001 prevede că toate operațiunile de prelucrare a datelor cu caracter personal de către instituții și organe ale UE, care pot prezenta riscuri specifice în legatură cu drepturile și libertățile persoanelor vizate, sunt supuse unei verificări prealabile de către Autoritatea Europeană pentru Protecția Datelor (AEPD).

În România, există o serie de reglementări legislative privind protecția și securitatea datelor: spre exemplu, Legea nr. 677 din 2001 (Capitolul V – *Confidențialitatea și securitatea prelucrărilor*); Legea nr. 311 din 22 mai 2002 (pentru utilizarea datelor personale în scopuri statistice, științifice sau istorice, serviciile de statistică oficială sunt obligate să asigure stocarea acestora în condiții de siguranță); Legea nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate (stipulează prevenirea accesului neautorizat la informațiile clasificate; protecția fizică a informațiilor, precum și a personalului necesar protecției informațiilor clasificate); Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice; Legea privind dreptul de autor și drepturile conexe nr. 8/1996 (stipulează obligația instituirii de măsuri tehnice de protecție a datelor informatice etc.

În SUA, se prezumă așa-numita "Duty of Care", care este definită ca o obligație pe care o persoană rezonabilă, în circumstanțe date, o consideră în acțiunile care îi vizează pe alții. Dacă aceste acțiuni nu sunt făcute într-o manieră atentă, responsabilă, acestea pot fi considerate neglijente și pot avea repercursiuni legale. Un număr de legi impun implementarea de măsuri de securitate informatică adecvată [spre exemplu, Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLB), Health Insurance Accountability and Portability Act (HIPAA) etc.], în

BCU IASI / CENTRAL UNIVERSITY LIBRARY

cazul în care aceste prevederi nu sunt respectate, existând consecinţe[109] (vezi, spre exemplu, cazul unei companii care nu a protejat adecvat reţeaua sa informatică împotriva atacurilor rezonabil previzibile şi a stocat informaţii personale într-o formă citibilă fără a fi necesar, care a fost investigată de autorităţile americane[110]). Măsurile de securitate informatică sunt aplicabile şi în ceea ce priveşte obligaţia părţilor de a produce, la cerere, documente care sunt relevante în disputele legale (*discovery*)[111].

Măsurile de securitate

Măsurile de securitate includ măsuri tehnice şi politici şi proceduri de folosire. **Măsurile tehnice** de securitate pot include *parole* (principalul mecanism de control al accesului la un sistem informatic), *sisteme anti-furt* (care detectează comportamentele suspecte, cum ar fi un număr excesiv de încercări de log-are nereuşite sau lipsa unei conectări la server-ul de monitorizare a furtului într-un interval predeterminat, declanşând dezactivarea respectivului calculator), *sisteme de control biometric*[112], *carduri cu cip* (de regulă, incriptate şi conţinând informaţii de acces), *sisteme de detectare a intruziunilor* (compuse din programe informatice care înregistrează sau capturează activitatea calculatoarelor şi a reţelelor de calculatoare şi furnizează utilitare capabile să genereze alarme automate despre condiţii periculoase şi să raporteze evenimentele pentru a ajuta administratorii de sistem să analizeze datele colectate în timpul sau după un incident de securitate), *programe anti-virus*, *firewall* (program care aplică politicile de trafic setate de administrator între o reţea informatică şi exterior) sau *sisteme criptografice*.

Pentru a *autentifica sursa* şi a *verifica integritatea* (nealterarea) unui conţinut[113], se folosesc şi semnături digitale, care protejează producătorii şi utilizatorii de programe informatice (fişiere .exe, .cab, .dll, .ocx, .msi, .xpi, sau .xap) când descarcă cod pe Internet sau reţele mobile (vezi, spre exemplu, *VeriSign*

---

109 Vezi T. J. Smedinghoff, *The Challenge of Electronic Data: Corporate legal obligations to provide information security*, Wall Street Lawyer, 10, 3, 1-10, 2006; V. R. Johnson, *Cybersecurity, identity theft, and the limits of tort liability*, South Carolina Law Review, Vol. 57, 2005.

110 *FTC Pursues Two Companies That Failed to Protect Employee Data from Reasonably Foreseeable Attacks*, The Computer & Internet Lawyer, Vol. 28, Number 7, July, 2011, p. 37.

111 Vezi H. L. Roitblat, A. Kershaw şi P. Oot, *Document categorization in legal electronic discovery: computer classification vs. manual review*, Journal of the American Society for Information Science and Technology, Vol. 61, Iss. 1, January, 70–80, 2010.

112 Aceste sisteme pot fi *Fiziologice*: bazate pe recunoaterea particularităţi biologice ale utilizatorilor, cum ar fi impresiuni digitale, recunoaştere facială (aceasta măsoară structura, forma şi proporţiile feţei utilizatorului, aspectele particulare fiind distanţele între ochi, nas sau gură, lungimea acestor organe şi unghiurile dintre acestea), geometria mâinii sau a venelor, analiza retinei sau a irisului; *Comportamentale*: bazate pe analiza vocii, dinamica semnării (inclusiv analiză tridimensională) sau dinamica tastării (informaţie detaliată privind modul în care fiecare tastă este apăsată de către un utilizator); *Multimodale*: bazate pe mai multe caracteristici fiziologice sau comportamentale pentru recunoaşterea individului.

113 În septembrie 2010, documente PDF cu o semnătură VeriSign validă furată au fost folosite pentru a transmite un contaminant informatic. Semnătura a permis acestor documente să treacă de măsurile de securitate ale sistemului Microsoft Windows – vezi cazul descris în Cisco, *2010 Annual Security Report*, 2011, p. 22.

BCU CLUJ / CENTRAL UNIVERSITY LIBRARY

Code Signing)[114]. Un certificat de tip "validare extinsă" (*extended validation* - EV) permite un proces de validare riguros care oferă garanţia că un document sau program nu a fost alterat sau compromis de o terţă parte. Certificatele de tip Secure Sockets Layer (SSL[115]) EV, pe de altă parte, oferă cel mai înalt nivel de criptare disponibil şi permit verificarea identităţii site-urilor web.

Semnarea digitală atestă că un document nu a fost alterat din momentul diseminării (adică, modificările nu sunt posibile fără a fi detectate). Certificatele pot fi emise pentru semnarea de documente sau date; certificare documente; executare conţinut dinamic incorporat într-un document certificat; executare JavaScript cu privilegii de nivel înalt incorporat într-un document certificat etc. Validitatea presupune că documentul nu a fost modificat, că identitatea semnatarului este validă şi că semnătura este datată (data calendaristică este marcată).

Semnarea documentelor poate fi manuală sau automată. În semnarea manuală, un individ sau un departament primeşte un token criptografic USB care stochează certificatul semnatarului, fiecare document fiind semnat individual. În cazul în care volumul de documente care se doreşte a fi semnate este mare, se foloseşte semnarea automată, metodă care presupune stocarea certificatului pe un modul de securitate fizică (*hardware security module*): se aplică o semnătură electronică pe document, după care este retrimis utilizatorului sau procesului[116]. În cazul în care se doreşte protejarea de date confidenţiale sau restricţionarea accesului la asemena date, se pot folosi sisteme de control a drepturilor şi privilegiilor de acces.

Cadrul pentru folosirea site-urile web pentru comerţ sau comunicaţii în condiţii de securitate se bazează pe certificate SSL. Aceste certificate digitale (documente care combină o cheie publică şi o identitate), în cazul în care sunt emise de autorităţi de încredere, permit utilizatorilor autentificarea site-urilor web, semnarea digitală a documentelor şi criptarea datelor senzitive şi sunt realizate pentru a fi folosite doar de titularul autentificat în certificat (autorităţile de certificare procesează interogările DNS prin intermediul registrului asociat)[117]. Aplicaţii client cum ar fi browser-ul web pot verifica dacă URL-ul site-ului este identic cu numele certificatului prezentat de site (de regulă, numele de domeniu întreg), în situaţiile în care browser-ul detectează nepotriviri va alerta utilizatorul printr-o casetă de dialog.

De remarcat că acest sistem de autentificare nu este lipsit de riscuri. Au existat cazuri de certificate SSL contrafăcute (spre exemplu, cazul <*.google.com>, care a fost disponibil pe web câteva săptămâni şi care furniza atacatorilor chei de criptare necesare pentru impersonarea unor servicii Google,

---

114 http://www.verisign.com/code-signing/information-center/why-sign-your-code/index.html.

115 Secure Sockets Layer (SSL) este un protocol de securitate criptografic, dezvoltat de Netscape Communications Corp. şi RSA Data Security, care vizează autenticitatea partenerilor şi integritatea şi confidenţialitatea datelor. Transport Layer Security (TLS) este un alt protocol criptografic, bazat pe SSL.

116 Vezi http://www.geotrust.com/signing-products/document-signing/enterprise/.

117 Vezi - - - - ; www.symantec.com/ssl -certificates.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

cum ar fi Gmail[118]), atacurile asupra companiilor care furnizează certificate digitale putând crea probleme semnificative (spre exemplu, cazul DigiNotar, în care peste 500 de certificate SSL frauduloase au fost emise[119]). Mai mult, este posibilă înşelarea clientului să vadă numele aşteptat, când, de fapt, numele de domeniu real în certificat este cel a unui site maliţios, aparţinând unui atacator (atacuri SSLStrip), putând duce la compromiterea confidenţialităţii datelor[120].

Politicile şi **procedurile** de folosire a sistemelor informatice reprezintă echivalentul legilor într-un sistem juridic[121] şi pot fi definite ca fiind formalizarea regulilor care trebuie respectate de toate categoriile de utilizatori ai sistemului informatic[122]. Politicile de securitate pot fi considerate şi o doctrină, o arhitectură, o organizare, un proces de control şi/sau un program de sensibilizare şi vizează securitatea la nivel fizic, operaţional, procedural, echipament, reţea şi aplicaţie. Conform SANS[123], politica de securitate protejează utilizatorii şi informaţiile, setează reguli privind comportamentul aşteptat din partea utilizatorilor, administratorilor şi managementului, autorizează monitorizarea sistemelor şi investigarea incidentelor de securitate[124], defineşte şi autorizează consecinţele încălcărilor şi vizează respectarea prevederilor legale[125].

2.7 Soluționarea litigiilor pe cale extrajudiciară

Disputele privind tranzacţiile electronice pot fi soluţionate în tribunale sau în afara lor. Deoarece disputele în tribunale pot fi lungi ca durată şi costisitoare, a apărut necesitatea unor mijloace de rezolvare în afara tribunalelor a disputelor privind tranzacţiile electronice, în speciale în ceea ce priveşte consumatorii. Astfel, Comisia Europeană a realizat o serie de recomandări privind rezolvarea alternativă a disputelor, după cum urmează:

- *Recommendation on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes,* COM (1998) 198;

---

118 Vezi SANS, *NewsBites*, Vol. XIII, Iss. 68, August 26, 2011.

119 Vezi J. Kirk, *Comodo Hacker Claims Credit for DigiNotar Attack*, IDG News Service, September 06, 2011.

120 Vezi L. Seltzer, *Spoofing Server-Server Communication: How You Can Prevent It*, 2009.

121 Vezi în A. Dutta şi K. McCrohan, *Management's role in Information Security in a Cyber Economy*, California Management Review, 45 (1), 2002.

122 Vezi M. Cavallari, *An Empirical Investigation On Beliefs And Perception About Compliance And Information Security Policy*, 2011.

123 Vezi SANS, *Information Security Policy - A Development Guide for Large and Small Companies*, 2011.

124 Vezi H.-C. Chu, D.-J. Deng şi H.-C. Chao, *An Ontology-driven Model for Digital Forensics Investigations of Computer Incidents under the Ubiquitous Computing Environments*, Wireless Personal Communations, 2011; S. L. Pfleeger, *Anatomy of an Intrusion*, IT Professional, Vol. 12, Iss. 4, 20–28, 2010; E. Casey, *Investigating sophisticated security breaches*, Communication of the ACM, 49(2) 48–54, 2006.

125 Vezi o abordare extensivă a politicilor şi procedurilor de securitate în Ioana Vasiu şi Lucian Vasiu, *Criminalitatea în cyberspaţiu*, Ed. Universul Juridic, Bucureşti, 2011.

BCU Cluj / Central University Library Cluj

- *Judicial Cooperation in Civil Matters: the Problems Confronting the Cross-Border Litigant*, COM (2000) 51 final;
- *Alternative Dispute Resolution in Civil and Commercial Matters*, COM (2002) 196 final;
- *European order for payment procedure and on measures to simplify and speed up small claims* litigation, COM (2002) 0746 final;
- *Alternative Dispute Resolution in Civil and Commercial Matters*, COM (2002) 196 final;
- *Recommendation on the principles for out-of-court bodies involved in the consensual resolution of consumer disputes*, OJ L109, 19/04/2001.

Conform Legii române a comerţului electronic (art. 20), furnizorii de servicii şi destinatarii pot supune litigiile născute între ei arbitrajului, în condiţiile prevăzute de lege, precum şi celorlalte căi extrajudiciare de soluţionare a litigiilor, prevăzute de codurile de conduită elaborate, potrivit art. 18.

2.8 Restricţii privind conţinutul informaţiilor furnizate

Există o serie de aspecte care trebuie luate în considerate la realizarea paginilor web, privind conţinutul lor. Printre cele mai importante aspecte privind responsabilitatea conţinutul paginilor web se numără cele care ating apartenenţa rasială, discriminarea sexuală, defăimarea, pornografia, competiţie neloială etc. În cazul furnizorilor de informaţii, art. 12-14 ale Directivei de Comerţ Electronic a UE disting între:

- *Transmitere* (*mere conduit*): furnizorul de servicii de informaţii nu va fi responsabil pentru conţinut ilegal dacă nu iniţiază transmisia, selectează recipienţii informaţiei sau modifică informaţia conţinută;
- *Păstrare temporară* (*caching*): furnizorul de servicii de informaţii nu va fi responsabil pentru conţinut ilegal păstrat temporar, cu scopul de a face mai eficientă transmiterea informaţiei la solicitare şi
- *Stocare* (*hosting*): furnizorul de servicii de informaţii va avea o răspundere limitată pentru conţinut ilegal stocat.

Conform Legii nr. 365/2002 (art. 14), dacă un serviciu al societăţii informaţionale constă în stocarea informaţiei furnizate de un destinatar al serviciului respectiv, furnizorul acelui serviciu nu răspunde pentru informaţia stocată la cererea unui destinatar, dacă este îndeplinită oricare din următoarele condiţii:

- Furnizorul de servicii nu are cunoştinţă despre faptul că activitatea sau informaţia stocată este nelegală şi, în ceea ce priveşte acţiunile în daune, nu are cunoştinţă despre fapte sau circumstanţe din care să rezulte că activitatea sau informaţia în cauză ar putea vătăma drepturile unui terţ;
- Având cunoştinţă despre faptul că activitatea sau informaţia respectivă este nelegală ori despre fapte sau circumstanţe din care să rezulte că activitatea ori informaţia în cauză ar putea vătăma drepturile unui terţ,

BCU IASI CENTRAL UNIVERSITY LIBRARY

furnizorul de servicii acţionează rapid în vederea eliminării sau a blocării accesului la aceasta.

2.9 Instrument de plată electronică

Noul Cod penal defineşte, în art. 180, "instrumentul de plată electronică" ca fiind "un instrument care permite titularului să efectueze retrageri de numerar, încărcarea şi descărcarea unui instrument de monedă electronică, precum şi transferul de fonduri, altele decât cele ordonate şi executate de către instituţii financiare". Prevederile acestui articol nu au corespondent în vechiul Cod penal, instituţia aceasta, însă, nu este nouă în peisajul legislativ românesc, ea fiind prezentă în legislaţia din România, după cum vom arăta mai jos, încă din anul 2002, iar legislaţia în europeană există o asemenea motivaţie încă din anul 1997 (aşadar, nu vorbim despre o "creaţie" a legiuitorului român, ci despre o preluare din cadrul legislativ comunitar, după cum vom arăta în mod amănunţit mai jos).

Instrumentele de plată reprezintă o componentă esenţială a sistemelor de plăţi. În general, plăţile electronice servesc ca mijloc de schimb, mijloc de plată, standard de valoare sau unitate de cont. Caracteristicile sistemelor de plată derivă din organizarea socioeconomică a societăţii în care acestea apar[126].

Progresele deosebite realizate în domeniile tehnologiei informaţiei şi al telecomunicaţiilor au revoluţionat societatea şi au schimbat radical relaţiile bancă-client şi chiar conceptul de bancă. Perioada modernă a dus la apariţia şi folosirea pe scară largă a unor forme noi de plăţi, care permit schimburi fără relaţii personalizate. Noile tehnologii au devenit atât un catalizator al marilor schimbări de care beneficiază consumatorii de servicii bancare, cât şi un mijloc de răspuns al băncilor pentru noile cerinţe. Mai mult, dezvoltarea comerţului electronic, în toate formele sale, a creat nevoi noi în domeniul financiar care, în multe cazuri, nu au putut fi efectiv îndeplinite prin sistemele tradiţionale de plată. În consecinţă, la nivel regional şi global s-au făcut eforturi pentru crearea şi dezvoltarea unui sistem complet şi complex de plăţi electronice[127].

Numărul de plăţi electronice efectuate este impresionant. În SUA, spre exemplu, conform Federal Reserve System[128], tranzacţiile anuale cu carduri de credit au crescut anul între 2009 şi 2012 cu 7,6%, ajungând la 26,2 miliarde în anul 2012. În China, în 2008, numărul de plăţi online a ajuns la 2,6 miliarde, cu o valoare totală de 263,6 trilioane yuan[129], iar în trimestrul II al anului 2013 numărul

---

[126] Vezi discuţii pe această temă în Wayne E. Baker şi Jason B. Jimerson, *The Sociology of Money, The American Behavioral, Sage Publications*, Jul/Aug, 1992, p. 678-693; Bill Maurer, *The Anthropology of Money, Annual Review of Anthropology*, 2006.

[127] Vezi European Central Bank, *E-payments in Europe – The Eurosystem's perspective*, 2002.

[128] Federal Reserve System, *Federal Reserve Payments Study*, 2013.

[129] L. Yunjie, C. Shumin & L. Wen, The Sustainable Development of ICT in China: The Rise and Future Development of the Internet, 2010.

total de plăți electronice a ajuns la 6,25 miliarde, cu o valoare totală de peste 251 trilioane yuani[130].

Cea mai asociată noțiune, când se vorbește despre "plăți", este cea de numerar (exprimată universal prin cuvântul *cash*) și se referă la bancnotele și monedele existente (dolari, euro, lei etc.). În sensul larg, prin "plăți" putem înțelege și contracte de recumpărare de tip *overnight*, acțiuni la fonduri mutuale de tip *money market*, obligațiuni de trezorerie lichide, opțiuni financiare de tip *futures* etc. În general, prin "instrument de plată electronică" se înțelege un instrument care permite titularului să efectueze retrageri de numerar, încărcarea și descărcarea unui instrument de monedă electronică, precum și transferul de fonduri, altele decât cele ordonate și executate de către instituții financiare.

Ca instituție, "plățile electronice" își găsesc reglementarea în dreptul afacerilor electronice (cu predilecție, în secțiunea dedicată comerțului electronic). Prin urmare, în mod firesc, în explicarea expresiei "instrument de plată electronică", noul Cod penal trebuia să țină seama de dispozițiile referitoare la definiția dată acestui tip de instrument în *Legea privind comerțul electronic* (Legea nr. 365/2002) în art. 1, precum și de dispozițiile BNR în domeniu, dispoziții care nu fac decât să preia cadrul legislativ comunitar în materie.

Legislația referitoare la plățile electronice și la securitatea plăților electronice s-a dezvoltat considerabil în ultimii ani, la nivel mondial și regional. O structură legală și un cadru adecvat al securității poate să susțină în mod propriu utilizarea sistemului de plăți electronice. Un cadru amplu și dinamic de politici și strategii în domeniul plăților electronice și al securității plăților electronice a fost elaborat în cadrul așa-numitului *Eurosystem*. Comisia Europeană a elaborat un cadru legal cuprinzător referitor la comerțul electronic, care constă în mai multe directive privitoare la comerțul electronic, la libera circulație a serviciilor online, moneda electronică și semnătura electronică.

Conținutul reglementării. În acest articol, legiuitorul penal a preferat să fie laconic, preluând din Legea nr. 365/2002 (care are la bază o reglementare europeană) o definiție care acoperă și instrumentul de plată cu acces la distanță și instrumentul de monedă electronică. De altfel, faptul că această definiție a instrumentului de plată electronică, pe care a utilizat-o legiuitorul român în acest articol, le include și pe celelalte două menționate mai sus este statuat în reglementarea europeană din anul 1997, care este, de fapt, prima sursă a acestei definiții.[131]

Apariția banilor electronici a reprezentat un pas decisiv în perfecționarea sistemelor de plăți și a adus importante avantaje clienților bancari prin facilitățile create de transmiterea rapidă a fondurilor și reducerea substanțială a costurilor tranzacțiilor, precum și autorităților monetare prin posibilitățile de reglare și

---

130 ChinaScope, China's mobile payments expand rapidly in 13Q2, 2013, disponibil la locația http://www.chinascopefinancial.com/news/article/27813-china-s-mobile-payments-expand-rapidly-in-13q2?lang=en.

131 A se vedea Reglementarea nr. 97/489/EC: *Commission Recommendation of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder*, publicată în Official Journal L. 208, 02/08/1997 (abrogată).

BCU IASI / CENTRAL UNIVERSITY LIBRARY

supraveghere a sistemului monetar şi, în special, al celui bancar. Revoluţia digitală a avut drept rezultat şi faptul că orice informaţie poate fi redusă în prelucrare la un flux digital, iar plata (banii, informaţie în general) devine doar o formă de informaţie digitală. Trecerea la sistemele electronice de plăţi a venit ca o consecinţă firească în evoluţia sistemului financiar–bancar.

În literatura de specialitate[132], "plăţile electronice" sunt definite ca o formă electronică, complet automatizată, de organizare a relaţiilor de plăţi între participanţii la o tranzacţie, pe baza unui set de reguli şi proceduri operatorii. Într-o variantă mai pragmatică, specialiştii de la Banca Mondială[133] consideră că operaţiunile financiare electronice reprezintă utilizarea mijloacelor electronice în scopul schimbului de informaţii, al transferului de simboluri sau reprezentări ale valorii şi a executării de tranzacţii într-un mediu comercial. Acest concept cuprinde patru canale: transferul electronic de fonduri, interschimbul de date electronice, transferul de instrucţiuni de plată şi confirmarea plăţii.

Legislaţia din România (Regulamentul BNR nr. 4/2002, privind tranzacţiile efectuate prin intermediul instrumentelor de plată electronică şi relaţiile dintre participanţii la aceste tranzacţii[134]), bazată pe cea comunitară, consideră că o "plată electronică" reprezintă orice operaţiune de plată iniţiată prin intermediul instrumentelor de plată electronică prin care se pot retrage sume în numerar, efectua plăţi pentru achiziţionarea de bunuri sau servicii, plata obligaţiilor către autorităţile administraţiei publice şi transferuri de fonduri între conturi. Tranzacţiile efectuate prin intermediul instrumentelor de plată electronică şi relaţiile dintre participanţii la aceste tranzacţii sunt reglementate de Regulamentul BNR nr. 4/2002, modificat şi completat de Regulamentul BNR nr. 6/2006.

Instrumentul de plată electronică poate fi atât un card sau un alt instrument de plată cu acces la distanţă, cât şi un instrument de plată de tip monedă electronică (*e-money*). Având în vedere faptul că articolul 180 a fost inclus pentru a servi la corecta înţelegere a calificărilor legale de la art. 250 C. pen. (*Efectuarea de operaţiuni financiare în mod fraudulos*) şi art. 251 C. pen. (*Acceptarea operaţiunilor financiare efectuate în mod fraudulos*), articole din noul capitol IV "Fraude comise prin sisteme informatice şi mijloace de plată electronice", Titlul II "Infracţiuni contra patrimoniului", este utilă şi necesară o definire a fiecărui concept-cheie utilizat de legiuitorul penal, nu doar o definiţie cu caracter general, cum este cea pe care a preferat-o legiuitorul nostru penal în acest articol.

Definirea clară, detaliată şi precisă este cerută şi de faptul că, în acest domeniu, nu se poate face trimitere la o singură reglementare (cum ar fi, spre exemplu, Legea nr. 365/2002), ci la un bogat şi deosebit de dinamic cadru

---

132 A se vedea o trecere în revistă a literaturii din domeniu în Charalampos Vassiliou, *Electronic payment systems and marketing: A literature review*, 2004.

133 Vezi definiţia citată în prezentarea lui Carlo F. Cattani, *Global practices in e-payment, International Trade Center*, UNCTAD/WTO, 2004.

134 Publicat în Monitorul Oficial, Partea I, nr. 503 din 12 iulie 2002, modificat şi completat de Regulamentul nr. 6 din 11 octombrie 2006, privind emiterea şi utilizarea instrumentelor de plată electronică şi relaţiile dintre participanţii la tranzacţiile cu aceste instrumente, publicat în Monitorul Oficial, Partea I, nr. 927 din 15 noiembrie 2006, intrat în vigoare la 15 noiembrie 2006.

legislativ european şi global, cu care legislaţia românească trebuie să se afle în armonie. Astfel, instrumentul de monedă electronică (*e-money*), în prezent definit la noi de Legea comerţului electronic şi de Regulamentul BNR menţionat mai sus, constituie o parte din Directiva 2009/110/EC, care completează şi modifică definiţii date de-a lungul timpului la nivel european, începând cu reglementarea din anul 1997 pe care am amintit-o mai sus. Mai mult, în această Directivă se subliniază importanţa unei definiţii precise a instrumentului de monedă electronică, definiţie unică, general acceptată la nivel european.

Pornind de la legislaţia europeană în materie (aflată, la rândul ei, în strânsă consonanţă cu reglementările de pe plan global), vom defini în continuare toţi termenii cheie legaţi de plăţile electronice. În conformitate cu legislaţia comunitară (mai precis, această legislaţie a fost tradusă aproape în întregime, în ceea ce priveşte tipurile şi definiţiile instrumentelor de plată electronică nefiind nici o diferenţă), Regulamentele BNR menţionate şi Legea nr. 365/2002 privitoare la comerţul electronic, se referă la următoarele tipuri de instrumente de plată electronică:

1. **Instrumente de plată la distanţă** (cardul, ordinul de plată electronic, cecul electronic);
2. **Instrumente de plată de tip monedă electronică** (portofelul electronic).

Pornind de la acelaşi cadru legislativ, suntem în măsură să definim tipurile de plăţi electronice enumerate mai sus şi care apar ca termeni-cheie în cuprinsul art. 250 şi art. 251 din noul Cod penal după cum urmează:

"Instrumentul de plată electronică" este instrumentul care permite utilizatorului să efectueze operaţiuni de tipul celor prevăzute la pct. 1 (art. 2) din Regulamentul BNR nr. 6/2006, şi anume:

• Retragerea de numerar, respectiv încărcarea şi descărcarea unităţilor valorice în cazul unui instrument de plată de tip monedă electronică, de la terminale precum distribuitoarele de numerar şi ghişeul automat de bancă (*Automated Teller Machine*, prescurtat ATM), de la ghişeele emitentului/băncii acceptante sau de la sediul unei instituţii, obligată prin contract să accepte instrumentul de plată electronică;

• Plata bunurilor sau a serviciilor achiziţionate de la comercianţii acceptanţi şi plata obligaţiilor către autorităţile administraţiei publice, reprezentând impozite, taxe, amenzi, penalităţi etc., prin intermediul imprinterelor, terminalelor de tip punct-vânzare (POS) sau prin alte medii electronice;

• Transferurile de fonduri între conturi, altele decât cele ordonate şi executate de instituţiile financiare, efectuate prin intermediul instrumentului de plată electronică.

Instrumentul de plată este şi rămâne proprietatea emitentului pe toată durata existenţei sale. Instrumentul de plată este pus la dispoziţia unei persoane fizice sau juridice numai pe baza unei cereri scrise adresate instituţiei.

Instrumentul de plată de tip monedă electronică (*e-money*) este instrumentul de plată electronică reîncărcabil sau nu, altul decât instrumentul de plată cu acces la distanţă, cum ar fi un chip-card, o memorie a unui calculator sau

un alt dispozitiv electronic, pe care sunt stocate electronic unități monetare, permițând deținătorului său să efectueze operațiunile prevăzute la pct. 1 (art. 2) din Regulamentul BNR nr. 6/2006 și care este acceptat la plată și de alte entități în afara emitentului, valoarea monetară stocată pe instrument fiind în mod obligatoriu egală cu suma primită de emitent de la deținător, respectiv utilizator, după caz.

În Directiva UE privitoare la moneda electronică (2009/110/EC[135]), prin "bani electronici"[136] se înțeleg valori monetare stocate electronic, inclusiv magnetic, așa cum sunt reprezentați de solicitările către emitent, emise la primirea de fonduri cu scopul efectuării de plăți definite conform punctului 5 al articolului 4 al Directivei nr. 2007/64/EC (Directiva Serviciilor de Plăți - DSP), acceptate de o persoană fizică sau juridică, alta decât emitentul. În aceeași Directivă, s-a statuat faptul că trebuie introdusă o definiție clară și cuprinzătoare a instrumentului de monedă electronică, pentru a o face neutră din punct de vedere tehnic și a permite includerea în definiție nu doar a produselor disponibile în acest moment, ci și a produselor care vor fi dezvoltate în viitor. De asemenea, această definiție ar trebui să acopere, prin urmare, toate situațiile în care un furnizor de servicii de plată emite o valoare preplătită în schimbul unor fonduri, care pot fi folosite pentru plată, fiind acceptată de terțe entități.

Instrumentul de plată cu acces la distanță este instrumentul ce permite deținătorului să aibă acces la fondurile aflate în contul său, prin intermediul căruia poate efectua plăți către un beneficiar sau alt gen de operațiuni de transfer de fonduri și care necesită, de obicei, un nume de utilizator și un cod personal de identificare (parolă) și/sau orice alt mecanism de autentificare. În categoria "instrumentelor de plată cu acces la distanță" sunt incluse, în special, *cardurile,* altele decât cele care fac parte din categoria instrumentelor de plată de tip monedă electronică (indiferent dacă sunt de debit sau de credit), precum și aplicațiile de tip *Internet-banking* și *home-banking*. În UE, cardurile de plată sunt cel mai popular instrument de plată *non-cash*, împreună cu transferurile de credit și *direct debit* reprezentând peste 90% din tranzacțiile *non-cash*[137].

Conform Regulamentului nr. 6/2006 al BNR (art. 2), *cardul bancar* emis de o instituție de credit este un instrument de plată electronică, respectiv un suport de informație standardizat, securizat și individualizat, care permite deținătorului său să folosească disponibilitățile bănești proprii dintr-un cont deschis pe numele

---

[135] Directivă a Parlamentului și Consiliului European din 16 septembrie 2009, care modifică Directivele nr. 2005/60/EC și nr. 2006/48/EC și elimină Directiva nr. 2000/46/EC din 18 septembrie 2000 privind inițierea, exercitarea și supravegherea prudențială a activității instituțiilor de bani electronici (text cu relevanță EEA).

[136] A se vedea și Council Regulation (EC) No 3604/93 și 97/489/EC: Commission Recommendation of 30 July 1997 privind tranzacțiile prin instrumente de plată electronică și în particular relația dintre emitent și deținător, Official Journal L 208, 02/08/1997, P. 0052 – 0058.

[137] Vezi European Commission, *Impact Assessment* - Accompanying the document Proposal for a directive of the European parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/UE and 2009/110/EC and repealing Directive 2007/64/EC and Proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions {COM(2013) 547 final}, {COM(2013) 550 final} {SWD(2013) 289 final}.

BCU Cluj Central University Library

său la emitentul cardului și/sau să utilizeze o linie de credit, în limita unui plafon stabilit în prealabil, deschisă de emitent în favoarea deținătorului cardului, în vederea efectuării uneia sau mai multora dintre următoarele operațiuni:

a) Retragerea sau depunerea de numerar de la terminale precum distribuitoarele de numerar și/sau ATM, de la ghișeele emitentului/instituției acceptante sau de la sediul unei instituții, obligată prin contract să accepte instrumentul de plată electronică, respectiv încărcarea și descărcarea unităților valorice în cazul monedei electronice;

b) Plata bunurilor achiziționate și/sau serviciilor prestate de comercianții acceptanți și/sau emitenți (de exemplu, plata serviciilor prestate de companii în domeniul telefoniei mobile, fixe, transmisii de date, servicii de televiziune și internet sau de către alți furnizori de utilități), precum și plata obligațiilor către autoritățile administrației publice, reprezentând impozite, taxe, amenzi, penalități etc., prin intermediul imprinterelor, terminalelor POS, ATM sau prin alte medii electronice;

c) Transferurile de fonduri.

Pe lângă operațiunile de transfer de fonduri, care conferă deținătorului instrumentului de plată cu acces la distanță posibilitatea transmiterii electronice a instrucțiunilor de debitare a contului curent propriu și a transcrierii mesajului dorit pe ordinul de plată, care va fi generat automat de sistem, deținătorul poate efectua și operațiuni de schimb valutar, poate constitui depozite și poate obține informații privind situația conturilor și a operațiunilor efectuate. Toate tranzacțiile efectuate sunt recepționate de bancă într-un server de comunicație și procesate printr-o tehnologie proprie de verificare a autenticității mesajului de plată, înainte de a fi transmise în sistemul informatic propriu.

În cazul aplicațiilor de tip *Internet-banking*, principiul de funcționare a acestor instrumente de plată cu acces la distanță se bazează pe tehnologia Internet, precum și pe sistemele informatice ale emitentului. În cazul aplicațiilor de tip *home-banking* principiul de funcționare a acestor instrumente de plată cu acces la distanță se bazează pe o aplicație informatică a emitentului, instalată la sediul deținătorului, pe o stație de lucru individuală sau în rețea. Regulamentul nr. 9/2007 privind monitorizarea sistemelor de plăți, a sistemelor de decontare a operațiunilor cu instrumente financiare și a instrumentelor de plată stabilește cadrul de desfășurare de către BNR a activității de monitorizare a sistemelor de plăți și a instrumentelor de plată, cu scopul de a identifica, evalua și diminua riscurile asociate acestora.

2.10 Identificare electronică

Definiții

Încrederea în identitatea electronică este esențială pentru dezvoltarea economică și socială. Regulamentul (UE) Nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei

1999/93/CE, care se aplică, cu unele excepţii, de la 1 iulie 2016, conţine următoarele definiţii:

- "identificare electronică" înseamnă procesul de utilizare a datelor de identificare a persoanelor în format electronic, reprezentând în mod unic fie o persoană fizică sau juridică, fie o persoană fizică care reprezintă o persoană juridică;
- "mijloace de identificare electronică" înseamnă o unitate materială şi/sau imaterială care conţine date de identificare personală şi care este folosită în scopul autentificării unui serviciu online;
- "date de identificare personală" înseamnă un set de date care permit stabilirea identităţii unei persoane fizice sau juridice sau a unei persoane fizice care reprezintă o persoană juridică;
- "sistem de identificare electronică" înseamnă un sistem pentru identificarea electronică în care sunt emise mijloace de identificare electronică pentru persoane fizice sau juridice sau persoane fizice reprezentând persoane juridice;
- "autentificare" înseamnă un proces electronic care permite confirmarea identificării electronice a unei persoane fizice sau juridice sau a originii şi integrităţii unor date în format electronic.

2.10.1 Semnături electronice

Cerinţele formale pentru tranzacţii legale variază de la o jurisdicţie la alta, precum şi de la o perioadă de timp la alta, însă o cerinţă importantă este cea privind *semnăturile*. Semnarea unui document este un act legal fundamental, aproape fiecarea document important fiind semnat[138]. Conform American Bar Association[139], semnătura serveşte următoarele scopuri:

- *Identitatea semnatarului/înscrisului*: O semnătură autentifică un semnatar şi un înscris prin identificarea semnatarului cu documentul semnat.
- *Ceremonial*: Actul semnării unui document asumă înţelegerea şi adoptarea semnificaţiei legale a respectivului document.
- *Aprobare*: În anumite contexte, o semnătură exprimă aprobarea de către semnatar a înscrisului şi intenţia acestuia ca documentul să aibă efecte legale.

O problemă majoră în cadrul afacerilor electronice este reprezentată de aplicarea sau respectarea tranzacţiilor[140]. Aceste probleme sunt semnificative şi prin prisma legislaţiilor care nu concordă în totalitate[141], aspect care a fost adresat

---

[138] C. Reed, *What is a Signature?*, The Journal of Information, Law and Technology, 2000.

[139] Vezi American Bar Association, *Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*, 1996.

[140] Vezi T. J. Smedinghoff, *The legal requirements for creating secure and enforceable electronic transactions*, 2002.

[141] Vezi T. J. Smedinghoff şi R. H. Bro, *Moving with change: Electronic signature legislation as a vehicle for advancing e-Commerce*, The John Marshall Journal of Computer & Information

de Directiva Europeană 1999/93/EC12 şi de UNCITRAL *Model Law on Electronic Signatures* care încearcă armonizarea legislaţiilor privind semnăturile electronice.

Conceptul legal de "semnătură" este unul larg, care recunoaşte orice semn făcut cu intenţia de a autentifica documentul marcat. În lumea digitală, conceptul de "semnatură" poate include şi imagini digitizate ale unor semnături de mână sau tastări de genul "/s/ Prenume Nume". Pentru realizarea scopului semnăturilor (excluderea falsificatorilor sau impostorilor, prevenirea modificării unilaterale a unui document, tranzacţii sau comunicaţii pentru realizarea *nonrepudierii*), trebuiesc îndeplinite următoarele:

- *Autentificarea semnatarului*: Semnătura trebuie să identifice clar cine a semnat documentul sau mesajul şi să facă practic imposibilă o semnătură identică pentru o altă persoană;
- *Autenticitatea documentului*: Semnătura trebuie să identifice ce s-a semnat, făcând practic imposibilă falsificarea sau alterarea documentului sau mesajului semnat sau a semnăturii fără a fi detectată.

Semnătura electronică nu este o scanare (digitizare) a unei semnături de mână ci un mecanism sofisticat care, implementat şi utilizat corect, poate soluţiona următoarele probleme legale de documentele, mesajele sau tranzacţiile electronice:

- Eliminarea sau dovedirea impostorilor sau a celor care pretind că au fost impersonaţi;
- Integritatea documentelor sau mesajelor, prin minimizarea riscului de modificare nedetectabilă a acestora; şi
- Satisfacerea unor cerinţe legale formale.

Semnătura electronică este, astfel, un mijloc de identificare şi de confirmare între părţi, adică un element de securitate. Tranzacţiile efectuate pe Internet exclud semnătura manuscriptă, care este înlocuită de semnătura electronică. În România, conform art. 4 al Legii nr. 455 din 18 iulie 2001, *semnătură electronică* reprezintă "date în formă electronică, care sunt ataşate sau logic asociate cu alte date în formă electronică şi care servesc ca metodă de identificare", în timp ce *semnătură electronică extinsă* reprezintă "acea semnătură electronică care îndeplineşte cumulativ următoarele condiţii:

- Este legată în mod unic de semnatar;
- Asigură identificarea semnatarului;
- Este creată prin mijloace controlate exclusiv de semnatar;
- Este legată de datele în formă electronică, la care se raportează în aşa fel încât orice modificare ulterioară a acestora este identificabilă".

Regulamentul (UE) Nr. 910/2014 al Parlamentului European şi al Consiliului din 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE, conţine următoarele definiţii:

Law, Vol. XVII, No. 3, Spring, 1999; N. Foggetti, *Electronic Signature: An Analysis of the Main European and International Legal Regulations*, Upgrade, V, No. 3, 2004.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

- "semnatar" înseamnă o persoană fizică care creează o semnătură electronică;
- "semnătură electronică" înseamnă date în format electronic, ataşate la sau asociate logic cu alte date în format electronic şi care sunt utilizate de semnatar pentru a semna;
- "semnătură electronică avansată" înseamnă o semnătură electronică ce îndeplineşte cerinţele prevăzute la articolul 26;
- "semnătură electronică calificată" înseamnă o semnătură electronică avansată care este creată de un dispozitiv de creare a semnăturilor electronice calificat şi care se bazează pe un certificat calificat pentru semnăturile electronice.

Conform Art. 25, (1) Unei semnături electronice nu i se refuză efectul juridic şi posibilitatea de a fi acceptată ca probă în procedurile judiciare doar din motiv că aceasta este în format electronic sau că nu îndeplineşte cerinţele pentru semnăturile electronice calificate.

(2) O semnătură electronică calificată are efectul juridic echivalent al unei semnături olografe.

(3) O semnătură electronică calificată bazată pe un certificat calificat eliberat de un stat membru este recunoscută drept semnătură electronică calificată în toate celelalte state membre.

Conform Art. 26, o semnătura electronică avansată îndeplineşte următoarele cerinţe:

(a) face trimitere exclusiv la semnatar;

(b) permite identificarea semnatarului;

(c) este creată utilizând date de creare a semnăturilor electronice pe care semnatarul le poate utiliza, cu un nivel ridicat de încredere, exclusiv sub controlul său; şi

(d) este legată de datele utilizate la semnare astfel încât orice modificare ulterioară a datelor poate fi detectată.

Folosirea semnăturilor electronice implică următorii paşi, executaţi fie de semnatar, fie de destinatarul mesajului semnat electronic:

(1) Utilizatorul obţine o pereche de chei criptografice unice (privată şi publică);

(2) Transmiţătorul pregăteşte un mesaj (spre exemplu, în forma unui mesaj de poştă electronică) pe un calculator;

(3) Transmiţătorul crează o semnătură electronică a mesajului, folosind un algoritm de criptare şi cheia privată;

(4) Transmiţătorul ataşează semnătura electronică la mesaj;

(5) Transmiţătorul expediază mesajul (criptat sau nu) şi semnatura electronică către un recipient;

(6) Recipientul foloseşte cheia publică a transmiţătorului pentru a verifica semnatura digitală (ceea ce certifică provenienţa mesajului de la transmiţător precum şi integritatea sa).

Aşadar, o "semnătură electronică" este o secvenţă de caractere creată de un calculator[142], o secvenţă neinteligibilă de biţi care rezultă din folosirea unei funcţii *hash*[143], pentru a crea un rezumat al mesajului comunicaţiei electronice, care apoi este criptat folosind un algoritm bazat pe o cheie publică şi o cheie privată (ultima folosită pentru verificarea semnăturii electronice). Un recipient care are cheia publică a transmiţătorului poate cu precizie să determine dacă secvenţa de biţi recepţionată a fost creată folosind cheia privată a presupusului semnatar şi dacă mesajul este nealterat din momentul în care a fost creată secvenţa respectivă de biţi.

O semnătură electronică verificată se presupune, din punct de vedere legal, în anumite circumstanţe, că îndeplineşte cerinţele de autenticitate, integritate şi nonrepudiere[144]. Astfel, o semnătură electronică poate fi o măsură de identificare a sursei comunicaţiei şi o modalitate de verificare a integrităţii acesteia, împiedicand, astfel, transmitatorul de la posibilitatea de a repudia respectiva comunicaţie sau tranzacţie. În timp ce folosirea criptografiei este una dintre caracteristicile principale ale unei semnături electronice, simplul fact că o semnătură electronică este folosită pentru a autentifica un mesaj conţinând informaţii într-o formă digitală nu trebuie confundat cu folosirea generală a criptografiei, pentru asigurarea confidenţialităţii.

Conform art. 5 al Legii nr. 455/2001, înscrisul în format electronic[145] căruia i s-a incorporat, ataşat sau asociat o semnătură electronică extinsă, bazată pe un certificat calificat nesuspendat sau nerevocat la momentul respectiv şi generată cu ajutorul unui mecanism securizat de creare a semnăturii este asimilat, în ceea ce

---

[142] Conform Legii române, "dispozitiv securizat de creare a semnăturii electronice" reprezintă acel dispozitiv de creare a semnăturii electronice care îndeplineşte cumulativ următoarele condiţii:
a) datele de creare a semnăturii, utilizate pentru generarea acesteia, să poată apărea numai o singură dată şi confidenţialitatea acestora să poată fi asigurată;
b) datele de creare a semnăturii, utilizate pentru generarea acesteia, să nu poată fi deduse;
c) semnătura să fie protejată împotriva falsificării prin mijloacele tehnice disponibile la momentul generării acesteia;
d) datele de creare a semnăturii să poată fi protejate în mod efectiv de către semnatar împotriva utilizării acestora de către persoane neautorizate;
e) să nu modifice datele în formă electronică, care trebuie să fie semnate, şi nici să nu împiedice ca acestea să fie prezentate semnatarului înainte de finalizarea procesului de semnare.

[143] Adică, o mapare algoritmică, sau o translatare a unei secvenţe de biţi într-o alta, în general un set mult mai mic (valoarea hash, valoarea de verificare a integrităţii, suma de control, cod de detectare a manipulării, rezumat al mesajului) astfel încât (1) o comunicaţie (sursă) generează acelasi rezultat hash de fiecare dată când algoritmul este executat folosind respectiva comunicaţie (sursă) ca intrare (*input*); (2) este computaţional nefezabil ca o cominicaţie să fie derivată sau reconstituită din rezultatul produs de algoritm şi (3) este computaţional nefezabil să fie găsite două comunicaţii care să producă acelaşi rezultat folosind algoritmul. Conform Hotărârii nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică, 'hash-code' este "funcţie care returnează amprenta unui document electronic" (art. 2).

[144] Vezi American Bar Association, *Digital Signature Guidelines*, 1996.

[145] Conform Legii nr. 455 din 18 iulie 2001 (Art. 4) un *înscris în formă electronică* reprezintă "o colecţie de date în formă electronică între care există relaţii logice şi funcţionale şi care redau litere, cifre sau orice alte caractere cu semnificaţie inteligibilă, destinate a fi citite prin intermediul unui program informatic sau al altui procedeu similar".

privește condițiile și efectele sale, cu înscrisul sub semnătură privată (vezi art. 5 al Legii nr. 455/2001). Conform art. 6 al Legii nr. 455/2001, înscrisul în format electronic căruia i s-a încorporat, atașat sau asociat o semnătură electronică, dar această semnătură nu este o semnătură electronică extinsă sau nu este bazată pe un certificat calificat sau nu este generată cu ajutorul unui mecanism securizat de generare a semnăturii, este asimilat, în ceea ce privește condițiile și efectele sale, cu începutul de probă scrisă, care poate fi completat cu alte mijloace de probă pentru a putea face dovada deplină a raportului juridic.

Conform art. 7 al Legii nr. 455/2001, înscrisul în format electronic căruia i s-a încorporat, atașat sau asociat o semnătură electronică, recunoscut de către acela căruia i se opune, sau care este privit de lege ca fiind recunoscut, are același efect ca actul autentic, între cei care l-au subscris și între cei care le reprezintă drepturile. Conform art. 7 al Legii nr. 455/2001, în cazurile în care, potrivit legii, forma scrisă este cerută ca o condiție de probă sau de validitate a unui act juridic, un înscris în format electronic îndeplinește această cerință dacă i s-a încorporat, atașat sau asociat o semnătură electronică extinsă, bazată pe un certificat calificat și generată prin intermediul unui mecanism securizat de creare a semnăturii.

Conform art. 16, alin. (3), modificat de Legea nr. 187/2012, "atunci când se utilizează un pseudonim, identitatea reală a titularului nu poate fi divulgată de către furnizorul de servicii de certificare decât cu consimțământul titularului sau la cererea unei autorități publice competente". Titularii de certificate sunt obligați să păstreze secretul datelor de creare a semnăturii și să solicite de îndată revocarea certificatelor în cazul în care au pierdut datele de creare a semnăturii, au motive să creadă că datele de creare a semnăturii au ajuns la cunoștința unui terț neautorizat sau informațiile esențiale cuprinse în certificat nu mai corespund realității (art. 45 al Legii nr. 455/2001).

Deși nu sunt lipsite de riscuri[146], semnăturile electronice reprezintă singura tehnologie care satisface cerințele legale referitoare la tranzacțiile electronice. Conform art. 8 al Legii nr. 455/2001, în cazul în care una dintre părți nu recunoaște înscrisul sau semnătura, instanța va dispune întotdeauna ca verificarea să se facă prin expertiză tehnică de specialitate, scop în care expertul sau specialistul este dator să solicite certificate calificate, precum și orice alte documente necesare, potrivit legii, pentru identificarea autorului înscrisului, a semnatarului ori a titularului de certificat.

---

[146] Vezi, spre exemplu, un caz de la sfârșitul anului 2012, în care s-a încercat folosirea unui certificat digital neautorizat pentru a impersona Google.com, pentru un atac de tip "man-in-the-middle", caz descris la locația http://www.wired.com/2013/01/google-fraudulent-certificate/?+wired%252Findex+%2528Wired%253A+Top+Stories%2529. Vezi, de asemenea, cazul în care VeriSign a furnizat unei persoane neautorizată două certificate digitale, care i-ar fi permis să se reprezinte în mod fals ca Microsoft și să furnizeze contaminanți informatici recipienților. Vezi alte discuții pe această temă în C. Ellison și B. Schneier, *Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure*, Computer Security Journal, XVI, 1, 1-8, 2000; B. Gelbord, *Signing Your 011001010: The problems of digital signatures*, Communications of the ACM, 43, No. 12, 27-28, 2000; A. Jøsang, D. Povey și A. Ho, *What You See is Not Always What You Sign*, Proceedings of AUUG2002, 2002; W. Kuechler și F. H. Grupe, *Digital signatures: A business view*, Information Systems Management, Winter, 19-28, 2003.

Pentru ameliorarea interoperabilității transfrontaliere a semnăturilor electronice și a identificării electronice, Comisia European a adoptat COM(2008) 798 final, *Plan de acțiune privind semnăturile electronice și identificarea electronică pentru facilitarea furnizării de servicii publice transfrontaliere pe piața unică.*

2.10.2 Sigilii electronice

Regulamentul (UE) Nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, conține următoarele definiții:

- „sigiliu electronic" înseamnă date în format electronic atașate la sau asociate logic cu alte date în format electronic pentru asigurarea originii și integrității acestora din urmă;
- „sigiliu electronic avansat" înseamnă un sigiliu electronic care îndeplinește cerințele prevăzute la articolul 36;
- „sigiliu electronic calificat" înseamnă un sigiliu electronic avansat care este creat de un dispozitiv de creare a sigiliilor electronice calificat și care se bazează pe un certificat calificat pentru sigiliile electronice;

Conform Art. 35, (1) Unui sigiliu electronic nu i se refuză efectul juridic și posibilitatea de a fi acceptat ca probă în procedurile judiciare doar din motiv că acesta este sub formă electronică sau că nu îndeplinește cerințele pentru sigiliile electronice calificate.

(2) Un sigiliu electronic calificat beneficiază de prezumția integrității datelor și a corectitudinii originii respectivelor date la care se referă sigiliul electronic calificat.

(3) Un sigiliu electronic calificat bazat pe un certificat calificat eliberat de un stat membru este recunoscut drept sigiliu electronic calificat în toate celelalte state membre.

Conform Art. 36, un "sigiliu electronic avansat" îndeplinește următoarele cerințele:

(a) face trimitere exclusiv la creatorul sigiliului;
(b) permite identificarea creatorului sigiliului;
(c) este creat cu ajutorul datelor de creare a sigiliilor electronice pe care creatorul sigiliului le poate utiliza sub controlul său, cu un nivel ridicat de încredere, pentru crearea sigiliilor electronice; și
(d) este legat de datele la care se raportează astfel încât orice modificare ulterioară a datelor poate fi detectată.

Conform Art. 37, (1) În cazul în care un stat membru solicită un sigiliu electronic avansat pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat membru recunoaște sigiliile electronice avansate, sigiliile electronice avansate bazate pe un

certificat calificat pentru sigilii electronice şi sigiliile electronice calificate care întrebuinţează cel puţin formatele sau metodele definite în actele de punere în aplicare menţionate la alineatul (5).

(2) În cazul în care un stat membru solicită un sigiliu electronic bazat pe un certificat calificat pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat membru recunoaşte sigiliile electronice avansate bazate pe un certificat calificat şi sigiliile electronice calificate care întrebuinţează cel puţin formatele sau metodele definite în actele de punere în aplicare menţionate la alineatul (5).

(3) Statele membre nu solicită un sigiliu electronic la un nivel de securitate mai ridicat decât cel al sigiliului electronic calificat pentru utilizarea transfrontalieră a unui serviciu online prestat de un organism din sectorul public.

(4) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referinţă ale standardelor pentru sigilii electronice avansate. În cazul în care un sigiliu electronic avansat îndeplineşte standardele respective, se presupune că acesta respectă cerinţele referitoare la sigiliile electronice avansate menţionate la alineatele (1) şi (2) de la prezentul articol şi la articolul 36. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 48 alineatul (2).RO L 257/104 Jurnalul Oficial al Uniunii Europene 28.8.2014

(5) Până la 18 septembrie 2015 şi ţinând cont de practicile, standardele şi actele juridice ale Uniunii existente, Comisia defineşte, prin intermediul unor acte de punere în aplicare, formate de referinţă ale sigiliilor electronice avansate sau metode de referinţă, în cazul în care sunt utilizate formate alternative. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 48 alin. (2).

2.11 Marcarea temporală

Momentul încheierii unui contract electronic sau al transmiterii unei comunicaţii electronice (dată şi oră) poate avea importanţă în comerţul electronic. Pentru a adresa acest aspect, a fost creat mecanismul marcării temporale, care implică o autoritate de marcare temporală (*Time Stamping Authority* - TSA), care adaugă o marcare temporală (*timestamp*) documentelor transmise de clienţi.

Marca temporală electronică (*electronic time stamp*) este o colecţie de date în formă electronică ataşată în mod unic unui document electronic. Ea certifică faptul că anumite date în formă electronică au fost prezentate la un moment de timp determinat furnizorului de servicii de marcare temporală[147]. Verificarea validităţii certificatelor digital ataşat se face folosind Online Certificate Status Protocol (OCSP). Certificatele revocate apar în Certificate Revocation List (CRLs).

---

[147] Vezi Legea nr. 451 din 1 noiembrie 2004 privind marca temporală. A se vedea şi Ordinul 492/2009 privind normele tehnice şi metodologice pentru aplicarea Legii nr. 451/2004 privind marca temporală.

BCU IAŞI / CENTRAL UNIVERSITY LIBRARY

Regulamentul (UE) Nr. 910/2014 al Parlamentului European şi al Consiliului din 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE,

(1) Unei mărci temporale electronice nu i se refuză efectul juridic şi posibilitatea de a fi acceptată ca probă în procedurile judiciare doar din motiv că aceasta este sub formă electronică sau că nu îndeplineşte cerinţele pentru marca temporală electronică calificată.

(2) O marcă temporală electronică calificată beneficiază de prezumţia corectitudinii datei şi orei pe care le indică şi a integrităţii datelor la care se raportează data şi ora indicate.

(3) O marcă temporală electronică calificată emisă într-un stat membru este recunoscută drept marcă temporală electronică calificată în toate statele membre.

Conform Art. 42, (1) O marcă temporală electronică calificată îndeplineşte următoarele cerinţe:

(a) asigură o legătură între dată şi oră şi date astfel încât să excludă în mod rezonabil posibilitatea ca datele să fie schimbate fără ca acest lucru să fie detectat;
(b) se bazează pe o sursă de timp precisă, legată de ora universală coordonată; şi
(c) este semnată utilizând o semnătură electronică avansată sau sigilată cu un sigiliu electronic avansat al prestatorului de servicii de încredere calificat sau printr-o metodă echivalentă.

Solicitarea unei mărci temporale de către un client TSA se face prin folosirea unui *software-client* (spre exemplu, aplicaţia clickSign[148]). TSA generează răspunsul de marcă temporală conform structurii TimeStampResponse, definită în RFC 3161, timpul de răspuns fiind de cel mult câteva secunde. Sistemele TSA fac posibilă verificarea online a mărcilor temporale, în mod normal chiar şi după expirarea certificatului cu care s-au semnat aceste mărci.

2.12 Dispute privind numele de domeniu Internet

În cadrul afacerilor electronice, un rol esenţial este jucat de *sistemul numelor de domeniu* (DNS). Încercând să ţină pasul cu eforturile regionale şi internaţionale în domeniu, România a înscris în strategia naţională în domeniul proprietăţii intelectuale (2003-2007)[149], în cadrul măsurilor privind armonizarea legislaţiei naţionale în domeniul proprietăţii intelectuale cu normele dreptului comunitar şi cu acordurile internaţionale la care România este parte, atât

[148] Vezi CertSign, *Instrucţiunile practice de marcare temporală*, 2009.

[149] A se vedea, Hotărârea Guvernului pentru aprobarea Strategiei Naţionale în domeniul proprietăţii intelectuale (2003-2007) nr. 1424 din 4 decembrie 2003 publicată în M. Of., p. I, nr. 905 din 18 decembrie 2003.

identificarea posibilelor conflicte între denumiri (mărci comerciale, nume personale, indicaţii geografice, denumiri ale soiurilor de plante), cât şi elaborarea de reglementări privind protecţia numelor de domeniu Internet.

Importanţa protecţiei numelor de domeniu Internet este indubitabilă şi a făcut obiectul unor ample cercetări[150]. Cu toate acestea, asigurarea unei protecţii efective şi rezolvarea disputelor în domeniu nu este deloc facilă[151]. Printre problemele cele mai complexe se numără:

- Distincţia dintre numele de domeniu şi mărcile înregistrate: Când, spre exemplu, poate o firmă să ceară daune pentru că un nume de domeniu seamănă cu una din mărcile sale de comerţ înregistrate?
- Stabilirea celor autorizaţi să administreze numele de domeniu: Ar trebui să fie organisme internaţionale sau organisme naţionale? În cazul în care sunt autorizate atât organismele internaţionale, cât şi cele naţionale, unde se trage linia de demarcaţie între ele?

Deoarece numele generice de domeniu sunt disponibile pentru înregistrare pe sistemul *primul venit=primul servit*, fără a fi necesar să se dovedească existenţa unor drepturi în mărcile de comerţ sau de servicii, este posibil ca unele nume de domeniu să fie înregistrate înainte ca deţinătorii mărcilor să realizeze sau exploateze valoarea lor comercială. Acest principiu, deşi asigură beneficii de netăgăduit, duce şi la numeroase dispute. Nu există acorduri care să permită celor care înregistrează nume de domeniu să elimine dosarele cu nume potenţial problematice, iar stabilirea deţinuătorului drepturilor asupra unui nume prezintă numeroase dificultăţi de ordin practic.

Ţinând seama de principiul mai sus enunţat, oricine poate să înregistreze orice nume de domeniu doreşte, condiţionat fiind de unicitatea numelor de domeniu secundare şi de limitarea înregistrărilor sub unele din domeniile de nivel superior (spre exemplu, o persoană particulară nu poate să creeze pentru sine un nume de domeniu sub domeniul generic *.int*, rezervat organismelor constituite în baza unui tratat internaţional). Apar destul de des probleme în ceea ce priveşte dreptul de a deţine un anumit nume de domeniu datorită modului de funcţionare al acestui principiu şi datorită faptului că unele cuvinte relativ comune sunt protejate ca mărci de comerţ. Problema este şi mai tare complicată de faptul că dreptul mărcilor de comerţ este aranjat predominant pe principii sectoriale, geografice şi naţionale, în timp ce Internet nu are astfel de graniţe[152].

---

150 Vezi, spre exemplu, W. W. Bettink, *Domain Name Dispute Resolution under the UDRP: The First Two Years*, European Intellectual Property Review, Vol. 24, 244-250, 2002; E. Katsh, J. Rifkin şi A. Gaitenby, *E-Commerce, E-Disputes, and E-Dispute Resolution: In the Shadow of "eBay Law"*, Ohio State Journal on Dispute Resolution, Vol. 15:3, 2000.

151 Dintr-o foarte lungă listă de dispute, considerăm ca interesante următoarele: Mattel, Inc. v. Adventure Apparel, 2001 U.S. Dist LEXIS 13885 (S.D.N.Y. 2001); Wal-Mart Stores, Inc. v. Walsucks and Walmarket Puerto Rico, WIPO Case No. D2000-0477 (2000); Virtual Works, Inc. v. Volkswagen of America, Inc., et al., 238 F.3d 262 (4th Cir., January 22, 2001); Porsche Cars North America, Inc. v. Porsche.net et al, 302 F.2d 248 (4th Cir. 2002); Kremen v. Cohen, No. 01-15899 (9th Cir. 2003).

152 Vezi o discuţie detaliată în A. M. Froomkin, *ICANN's "Uniform Dispute Resolution Policy"-Causes and (partial) cures*, Brooklyn Law Review, Vol. 67 (3), 605, 2002.

Numele de domeniu Internet sunt protejate de legile privind mărcile de comerț[153]; de obicei, numele de domeniu sunt folosite pentru a identifica locația web a unei anumite companii sau un produs sau serviciu al acesteia[154]. Considerăm că asimilarea numelor de domeniu cu termenul de *brand* sau cu cel de marcă de comerț nu este cea mai bună soluție[155], datorită faptului că marca de comerț are un caracter multiplu, iar numele de domeniu au un caracter unic. Spre exemplu, în SUA, pe lângă "Apple Computers", mai multe companii au înregistrat "Apple" ca marcă de comerț. Chiar dacă am considera, prin absurd, că una din aceste companii ar fi înregistrat numele de domeniu <Apple.com> înaintea companiei Apple Computers, asta nu înseamnă că ar fi încălcat dreptul la marca de comerț a acestei firme.

În general, actul de înregistrare a unui nume de domeniu cu scopul de a-l vinde sau licenția este perfect legal. Pe de altă parte, un "cyberpirat" care înregistrează un nume de domeniu care reprezintă sau incorporează mărci de comerț înregistrate cu intenția de a vinde domeniu deținătorului mărcii pentru profit sau de a folosi domeniul cu intenția de a beneficia de pe urma valorii mărcii de comerț acționează ilegal.

Dezvoltarea unui nume de domeniu și dezvoltarea unui *brand* (marcă) servesc unui scop similar. În lumea digitală, însă, un nume de domeniu își dublează funcția în momentul în care utilizatorii încep să recunoasca numele de domeniu ca "identificarea" unui anumite locații web. În consecință, numele de domeniu operează ca mărci de comerț și generează beneficii ca în cazul recunoașterii unei mărci de comerț, de aceea este posibilă înregistrarea lor ca mărci de comerț.

De cele mai multe ori, disputele referitoare la numele de domeniu se nasc în urma înregistrări de nume de domeniu care sunt sau conțin nume identice, asemănătoare sau derivate din nume de mărci universal recunoscute, efectuate cu scopul de a profita cu rea-credință. S-au înregistrat cazuri în care au fost înregistrat nume de domeniu, oferite ulterior contra cost tocmai celor care erau îndreptățiti să dețină aceste nume de domeniu. Această practică a fost declarată ilegală și este cunoscută sub numele de "cybersquatting"[156].

---

[153] Vezi o discuție despre conflictul dintre numele comercial și marcă în N. Burchel și M. Gavenea, *Conflictul nume comercial – marcă*, Revista Română de Dreptul Proprietății Intelectuale, III, 1 (6), 71-76, 2006.

[154] Privind folosirea efectivă a unei mărci, a se vedea o discuție în M. Ionescu, *Folosirea mărcii în comerțul electronic constituie folosire efectivă?*, Revista Română de Dreptul Proprietății Intelectuale, III, 1 (6), 106-123, 2006. Privind proba folosirii mărcii, a se vedea S. Florea, *Proba folosirii mărcii*, Revista Română de Dreptul Proprietății Intelectuale, III, 4 (9), 119-129, 2006.

[155] Puncte de vedere asemănătoare au fost exprimate de numeroși autori: J. A. Katz, și J. A. Carnahan, *Battling the "CompanyNameSucks.com" cyberactivists*, Intellectual Property & Technology Law Journal, Vol. 13, No. 3, March, 1-7, 2001; G. P. Albert, Jr., *Right on the Mark, Defining the Nexus Between Trademarks and Internet Domain Names*, 15 John Marshall Law Review 277, 278, 1997.

[156] Vezi, spre exemplu, M. E. Searing, *"What's in a domain name?" A critical analysis of the national and international impact on domain name cybersquatting*, Washburn Law Journal, 40

BCU IASI CENTRAL UNIVERSITY LIBRARY

Cybersquatterii profită de pe urma principiului de atribuire a numelor de domeniu (*primul venit=primul servit*), ale cărui neajunsuri le-am criticat mai sus. Operaţiunea este una dintre cele mai facile: ei înregistrează nume de mărci de comerţ sau nume ale unor persoane cunoscute ori nume ale unor firme cu care ei nu au nici o legătură. Profitând de faptul că o asemenea înregistrare nu este scumpă sau dificilă, aceştia pot să ajungă să înregistreze numeroase astfel de nume de domenii.

Din cele arătate mai sus, nu trebuie să se tragă concluzia că este ilegal comerţul cu nume de domeniu, dacă nu sunt implicate mărci înregistrate. Datorită faptului că numele de domeniu sunt extrem de dorite pentru scopuri de afaceri, acest comerţ poate fi considerat o oportunitate extrem de profitabilă. Spre exemplu, numele de domeniu <Sex.com> a fost vândut în 2010 pentru o suma de 13 milioane dolari; <Business.com> a fost vândut în 1999 pentru o suma de 7,5 milioane dolari; <Wine.com> a fost vândut pentru 3 million dolari în 1999[157]. Acest tip de comerţ nu este ilegal, atât timp cât înregistrarea şi folosirea acelui nume nu trebuie să stârnească o posibilă confuzie cu o marcă înregistrată.

Posibilitatea ca unele nume de domeniu să fie exprimate prin cuvinte sau fraze cu caracter comun, de largă utilizare, este reală. Protecţia acestor nume de domeniu va fi mai complicată decât în cazul existenţei unui nume de domeniu alcatuit din cuvinte distincte. Când numele de domeniu ales conţine marca unui terţ, atunci acest caracter speculativ poate veni în contradicţie cu mecanismele de protecţie pentru mărci de comerţ deoarece se poate considera că se profita de beneficiile asociate unor asemenea mărci.

În SUA, Congresul a adoptat o lege specială numită *The United States Anticybersquatting Consumer Protection Act* (ACPA). În mare parte această lege este menită să protejeze interesele companiilor împotriva persoanelor care acţionează cu rea credinţă, înregistrează un nume de domeniu care este similar sau poate conduce la confuzii cu o marcă de comerţ existentă. ACPA stipulează următoarele criterii pentru determinarea "relei credinţe", cu intenţia de a profita de pe urma folosirii unui nume de domeniu:

- Registrantul are drepturi de marcă de comerţ sau alte drepturi de proprietate intelectuală în domeniul disputat;
- Numele de domeniu este numele legal al registrantului sau un nume după care acesta este cunoscut;
- Registrantul a folosit anterior numele de domeniu pentru a identifica bunuri sau servicii *bona fide*;
- Registrantul foloseşte numele de domeniu pentru scopuri non-comerciale;
- Registrantul are intenţia de a atrage consumatori de la locaţia deţinătorului mărcii de comerţ pentru câştiguri comerciale sau pentru a dilua sau afecta negativ marca de comerţ prin inducerea idei că locaţia registrantului este sponsorizată de deţinătorul mărcii de comerţ;

(1), 2000; G. J. Johnson şi colab., *Cybersquatting: the latest challenge in Federal Trademark Protection*, Duke Law & Technology Review, 2001.

[157] Vezi Business Insider, *The 25 Most Expensive Domain Names*, 2012 (http://www.businessinsider.com /the-20-most-expensive-domain-names-2012-12?op=1).

BCU IASI CENTRAL UNIVERSITY LIBRARY

- Registrantul oferă numele de domeniu spre vânzare deţinătorului mărcii de comerţ, cu intenţia de a profita din vânzare, fără a intenţiona folosirea numelui de domeniu *bona fide*;
- Registrantul foloseşte informaţii de contact false la înregistrarea numelui de domeniu;
- Registrantul a achiziţionat mai multe nume de domeniu despre care ştie că sunt similare unor mărci de comerţ faimoase sau distinctive;
- Marca folosită este faimoasă sau distinctivă.

ACPA are şi o secţiune care face referire la persoanele cunoscute. Acestora le este recunoscut dreptul de a acţiona în instanţă pe oricine înregistrează numele lor ca nume de domeniu la nivel secundar, cu scopul de a revinde aceste nume de domeniu pentru profit[158]. Conform ACPA, pentru a demonstra că este o situaţie de tipul "reverse domain name hijacking"[159] împotriva deţinătorului unei mărci de comerţ care "se întinde prea mult" (*overreaching*), registrantul trebuie să arate următoarele[160]:

- este registrantul unui nume de domeniu;
- numele de domeniu înregistrat a fost suspendat, dezactivat sau transferat [conform 15 U.S.C. § 1114(2)(D)(ii)(II)];
- deţinătorul mărcii care a determinat suspendarea, dezactivarea sau transferul numelui de domeniu este notificat de existenţa acţiunii; şi
- folosirea sau înregistrarea domeniului de către înregistrant nu este ilegală conform Legii Lanham.

În ţara noastră, dacă o persoană foloseşte un asemenea nume pentru a comercializa bunuri sau servicii care sunt în concurenţă cu bunurile sau serviciile deţinătorului mărcii, acţiunile sale încalcă dreptul la marcă al deţinătorului de drepturi în domeniu şi va răspunde conform prevederilor Legii nr. 84/1998 privind mărcile şi indicaţiile geografice[161].

Din cele prezentate, se observă că, în afara cazului în care se încalcă dreptul la marcă, înregistrările de nume de domeniu ridică probleme atunci când există cel puţin doi deţinători ai unei mărci de comerţ[162] sau când se manifestă

---

158 În California, spre exemplu, *Cyberpiracy Act* a introdus, în anul 2000, protecţie extinsă pentru numele personale.

159 *Reverse domain name hijacking* (numit şi *reverse cybersquatting*) este acţiunea prin care un deţinător de marcă încearcă să obţină un nume de domeniu prin pretenţii false împotriva deţinătorului de drept al respectivului nume de domeniu.

160 A se vedea cazul Barcelona.com v. Excelentisimo Ayuntamiento De Bardelona, 330 F.3d 617, 626 (4th Cir. 2003), discutat în Ryan R. Owens, *Domain-Name Dispute-Resolution after Sallen v. Corinthians Licenciamentos & Barcelona.com, Inc. v. Excelentisimo Ayuntameiento De Barcelona*, Berkeley Technology Law Journal, Vol. 18 (1), 257-274, 2003. Legea Lanham stipulează faptul că un termen care desemnează o zonă cu semnificaţie geografică nu poate fi înregistrată ca marcă de comerţ decât dacă a dobândit un înţeles secundar. În acest caz, "Barcelona" s-a considerat că trebuie tratat ca un termen our geografic desciptiv, care nu permite protecţie prin marcă de comerţ.

161 Republicată în Monitorul Oficial, Partea I, nr. 337 din 8 mai 2014.

162 Privind dificultăţile de rezolvare a disputelor care implică părţi cu interese legitime privind mărcile în numele de domenii, a se vedea şi Jacqueline D. Lipton, *A winning solution for*

BOLYAI UNIVERSITY LIBRARY

fenomenul de cybersquatting. Disputele care implică deţinătorii unor mărci de comerţ identice sunt dificil de rezolvat. Într-un caz elocvent, compania Nissan Motors a dat în judecata compania Nissan Computer, atât pe temeiul încălcării dreptului la marcă, cât şi pe temei de cybersquatting[163].

În 1994, Nissan Computer a înregistrat numele de domeniu *nissan.com*, pentru a oferi informaţii şi servicii referitoare la calculatoare. După ce a descoperit că pe site-ul în cauză se faceau reclame la mai multe produse pentru autoturisme, Nissan Motors a dat în judecata compania Nissan Computer. Instanţa a decis, în parte, în favoarea companiei Nissan Motors, pe temeiul încălcării dreptului la marcă, a dispus interzicerea afişării de informaţii şi a obligat compania deţinătoare a numelui de domeniu (Nissan Computer) să afişeze un anunţ de disociere (*disclaimer*) pe site-ul respectiv. Mai mult, prin aceeaşi decizie Nissan Computer a fost obligată să înceteze orice acţiune care ar putea fi considerata prejudiciabilă pentru Nissan Motors.

Pentru a preveni înregistrările abuzive, unele organizaţii înregistrează numeroase nume de domeniu. Spre exemplu, Consorţiul Parmigiano Reggiano (*Consorzio del Formaggio Parmigiano Reggiano*), organizaţie nonprofit înfiinţată în 1934, responsabilă, printre altele, de protejarea brânzei PARMIGIANO-REGGIANO[164], incluzând denumirea şi traducerile sale, supervizarea producţiei şi promovarea mărcii şi a indicaţiei geografice, a înregistrat numeroase nume de domeniu: <www.parmigiano-reggiano.it>; <www.parmigiano-reggiano.com>; <www.parmesan.it>; <www.parmigiano.it>; <www.parmigianoreggiano.eu>; <parmigianoreggiano.com>; <parmigiano-reggiano.cn>; <www.parmigiano-reggiano.asia>, <www.parmigianoreggiano.com>[165].

Rezolvarea disputelor privind numele de domeniu la OMPI

În iulie 1998, Organizaţia Mondială a Proprietăţii Intelectuale [*World Intellectual Property Organization* (WIPO)] a început un proces extensiv de consultări (cunoscut sub denumirea *the WIPO Internet Domain Name Process*), pentru a adresa în mod efectiv problema disputelor privind numele de domenii Internet. Scopul acestui proces a constat în transmiterea de recomandări către ICANN, corporaţia care se ocupă de managementul tehnic al sistemului numelor

---

YouTube and Utube? Corresponding trademarks and domain name sharing, Harvard Journal of Law & Technology, Vol. 21, 2, Spring, 509-545, 2008.

163 Nissan Motor Co. v. Nissan Computer Corp., 378 F.3d 1002 (9th Cir. 2004). Vezi o discuţie detaliată a cazului în Bruce C. Piontkowski şi Matthew S. Kenefick, *Nissan Motor Co. v. Nissan Computer Corp.: The Point at Which Fame Is Determined Under the Federal Trademark Dilution Act*, Santa Clara High Technology Law Journal, 21 (3), 2004.

164 *Parmigiano Reggiano* este, din 1996, o denumire de origine protejată [*Protected Designation of Origin* (PDO)] în toată UE, in virtutea Council Regulation (EC) No. 510/2006. Brânza, produsă prima dată de călugari acum 1000 ani, generează vânzări anuale de circa 2 miliarde euro – vezi http://www.parmigiano-reggiano.it/come/guida_parmigiano_reggiano/parmigiano_reggiano_cifre.aspx

165 Vezi http://www.wipo.int/ipadvantage/en/details.jsp?id=3664.

de domeniu[166]. Pentru rezolvarea disputelor privind numele de domeniu, a fost creat WIPO Arbitration and Mediation Center[167].

Acest organism a creat instrumentul cunoscut sub denumirea *Uniform Domain Name Dispute Resolution Policy* (pe scurt, UDRP *Policy*, adoptat de ICANN în august 1999[168]) şi instrumentul *Rules for Uniform Domain Name Dispute Resolution Policy* (pe scurt, UDRP *Rules*, aprobat de ICANN în octombrie 1999[169]). Ulterior, centrul WIPO a realizat *Supplemental Rules for the Uniform Domain Name Dispute Resolution Policy* (UDRP), cu aplicare din 1 decembrie 1999. Aceste instrumente furnizează remedii eficiente împotriva înregistrării abuzive a numelor de domeniu[170].

Chiar în primul său an de activitate propriu-zisă (2000), Centrul de Arbitraj şi Mediere al Organizaţiei Mondiale a Proprietăţii Intelectuale a administrat 1840 de dispute privitoare la numele de domeniu Internet, dând decizii în 1000 de cazuri[171]. Din decembrie 1999 până la începutul anului 2014, Centrul WIPO a administrat circa 28.000 cazuri pe baza UDRP[172]. Pentru a obţine anularea sau transferul unui nume de domeniu, trebuiesc dovedite următoarele elemente, conform paragrafului 4(a) al *Policy*:

(i) Numele de domeniu disputat este identic sau similar de o manieră a fi confundat cu mărci de comerţ sau de servicii în care reclamantul are drepturi;

(ii) Respondentul nu are drepturi sau interese legitime în numele de domeniu respective; şi

---

166 ICANN a fost formată în octombrie 1998 cu scopul de a organiza, la nivel internaţional., sistemul numelor de domenii (*DNS*), alocarea adreselor IP, managementul sistemului "rădăcină" (*the root server*) şi coordonarea protocolului de asignare a numerelor.

167 Vezi detalii în WIPO, *Arbitration and Mediation Rules* (2002); WIPO, *Dispute Resolution for the 21st Century*, 2004.

168 Vezi UDRP *Policy, adoptată de toate* organizaţiile care gestionează numele de domenii *terminate în .com, .net şi .org*, precum şi unele domeniu ccTLD, disponibilă la locaţia http://archive.icann.org/en/udrp/udrp-policy-24oct99.htm.

169 Vezi UDRP *Rules* la locaţia www.icann.org/udrp/udrp-rules-24oct99.htm

170 Pentru arbitrarea disputelor privind numele de domenii Internet, există şi alte organisme, cum ar fi NAF (*The National Arbitration Forum* – Minneapolis, USA), ADNDRC (*Asian Domain Name Dispute Resolution Centre* – Beijing and Hong Kong, China) sau CPR (*CPR Institute for Dispute Resolution* - Asia). O dispută poate fi, de asemenea, rezolvată într-un tribunal care are jurisdicţie [vezi, spre exemplu, Resorts of Pinehurst, Inc. v. Pinehurst National Corp., 47 U.S.P.Q.2d 1465, 148 F.3d 417 (4th Cir. 07/15/1998)].

171 Centrul de Arbitraj şi Mediere al OMPI (*WIPO Arbitration and Mediation Center*) a devenit liderul mondial în domeniul furnizării de rezoluţii în disputele referitoare la numele de domenii, putere ce i-a fost conferită de *Uniform Domain Name Dispute Resolution Policy* (UDRP). Această reglementare inovativă, adoptată în 1999 de către *Internet Corporation for Assigned Name and Numbers* (ICANN) le oferă deţinătorilor de drepturi în domeniul mărcilor de comerţ un remediu administrativ împotriva înregistrărilor şi utilizărilor cu rea credinţă de către terţi a numelor de domeniu ce corespund cu mărcile de comerţ ocrotite. A se vedea, pentru amănunte, World Intellectual Property Organization, *Annual Report 2000*, p. 29; CPR Institute for Dispute Resolution, www.cpradr.org/ICANN_Menu.htm; eResolution, www.eresolution.ca/services/dnd /arb.htm; The National Arbitration Forum, www.arbforum .com/domains/; World Intellectual Property Organization - Arbitration and Mediation Center, www.arbiter.wipo.int/domains/.

172 WIPO, *Update on trademark-related aspects of the domain name system*, 2014.

(iii) Numele de domeniu a fost înregistrat și este folosit cu rea credință.

Conform UDRP, se poate decide transferul sau anularea numelui de domeniu sau rejectarea plângerii. În situațiile în care un registrat de nume de domeniu demonstrează că procesul de arbitrare este folosit abuziv sau pentru a hărțui registrantul, solicitarea de transfer a numelui de domeniu va fi respinsă[173]. Disputele privind noile gTLD sunt arbitrate conform *New gTLD Dispute Resolution Procedure* și *Rules for New gTLD Dispute Resolution for Existing Legal Rights Objections* ("WIPO Rules for New gTLD Dispute Resolution"), din anul 2011.

Un caz interesant, adus în 2013 la Comisia de arbitraj și mediere de la WIPO, a fost *Pinterest, Inc. v. Amazon EU S.à.r.l* (Case No. LRO2013-0050), privind aplicația pentru un nou gTLD transmisă către ICANN, anume .pin. Comisia de arbitraj a decis că utilizarea de către Amazon a domeniului .pin:

(i) nu crează o confuzie impermisibilă între gTLD și logo-ul Pinterest, cuvântul PINTEREST sau marca PIN IT; și

(ii) nu folosește un avantaj nemeritat al caracterului distinctiv sau reputației acestor mărci; și

(iii) nu afectează nejustificat caracterul distinctiv și reputația acestor mărci.

Sistemul *Uniform Rapid Suspension* (URS) este un nou mecanism de protejare a drepturilor creat pentru noile gTLD și permite deținătorilor de mărci o alternativă rapidă și ieftină[174] la UDRP în cazurile de încălcare evidentă a mărcilor. O plângere URS trebuie să arate că:

(1) Numele de domeniu înregistrat este identic sau similar de o manieră care crează confuzie cu o marcă:
   (a) pentru care reclamantul deține o înregistrare națională sau regională care este în utilizare curentă; sau
   (b) care a fost validată printr-o decizie a unei instanțe de judecată; sau
   (c) care este specific protejată de un tratat sau statut activ la momentul în care plângerea este depusă;

(2) Cel care a înregistrat domeniul nu are nici un drept sau interes legitim și

(3) Domeniul a fost înregistrat și este folosit cu rea credință.

Singurul remediu conform URS este *suspendarea* numelui de domeniu. Acest mecanism nu se aplică la numele ccTLD (spre exemplu, .us sau .ro) și nici la gTLDs: .aero, .arpa, .asia, .biz, .cat, .com, .coop, .edu, .gov, .jobs, .info, .int, .mil, .mobi, .museum, .name, .net, .org, .post, .pro, .tel, .travel și .xxx. În primul caz arbitrat conform URS, care a implicat numele de domeniu <facebok.pw>, identic sau similar cu marca FACEBOOK, în care respondentul nu are drepturi sau interese legitime, fiind folosită pentru a obține câștiguri financiare, numele de

---

[173] Vezi, spre exemplu, Goldline International, Inc. v. Gold Line, Case No. D2000-1151 (WIPO, Jan. 4, 2001).

[174] Costul unei plângeri este de \$300-\$500, față de \$1,000-\$7,000 pentru plângeri UDRP.

domeniu a fost suspendat[175]. Procedura usRS, pe de altă parte, se aplică la numele din domeniul .us[176].

Pentru a proteja mărcile în contextul noilor gTLDs, ICANN a creat un program numit "Trademark Clearinghouse" (TMC sau TMCH), constând dintr-un registru global care permite includerea mărcilor înregistrate, protejate de tratate sau validate legal, folosit în *Trademark Claims* şi *Sunrise Services*, impuse în toate noile gTLDs, pentru a informa deţinătorii de mărci despre posibile încălcări ale drepturilor. Circa 33000 mărci au fost înregistrate până în 16 septembrie 2014[177]. "Legal Rights Objections" (LRO) este o altă procedură, realizată în colaborare de WIPO şi ICANN, prin intermediul căreia deţinătorii mărcilor şi organizaţii interguvernmentale pot obiecte la aplicaţia unei terţe părţi pentru un nou TLD.

Arbitrarea disputelor privind numele de domeniu care implică mărci este, în unele cazuri, complexă. Pentru a ilustra modul în care sunt rezolvate asemenea dispute, am selectat şi rezumăm în continuare cazuri WIPO. Cazurile selectate acoperă numeroase domenii de activitate, modalităţi de înregistrare abuzivă a unor nume de domeniu şi firme din diverse jurisdicţii, pentru a da o imagine cuprinzătoare a problemei.

2.12.1 Cazuri privind mărci

Costamar Travel Cruises & Tours, Inc. v. Maya World, S.C. (No. D2006-0003)

Costamar Travel Cruises & Tours, Inc., Ft. Lauderdale, SUA a reclamat Maya World S.C., Cancun, Mexic, pentru folosirea numelui de domeniu <costamartravel.com>. Costamar Travel Cruises & Tours, Inc. deţine marca de comerţ COSTAMAR, înregistrată în SUA, COSTAMAR TRAVEL DE MEXICO SA de CV în Mexic şi COSTAMAR TRAVEL S.A. în Peru. Costamar Travel Cruises & Tours, Inc. are peste 30 de birouri în SUA, altele în Peru, Ecuador, Colombia şi Brazilia şi a folosit marca de comerţ COSTAMAR TRAVEL de peste 25 de ani, fiind o marcă de comerţ bine cunoscută în domeniul serviciilor turistice în cadrul comunităţii de limbă spaniolă.

Numele de domeniu în dispută este identic cu COSTAMAR şi similar de o manieră a fi confundat cu COSTAMAR TRAVEL. Costamar Travel Cruises & Tours, Inc. a susţinut că respondentul nu are drepturi sau interese legitime în numele de domeniu deoarece nu îl foloseşte ca marcă de comerţ sau într-o altă manieră, diferită de nume de domeniu. Mai mult, numele de domeniu nu descrie un atribut al serviciilor oferite de respondent, cunoscut ca "Mexico Hoy". Costamar Travel Cruises & Tours, Inc. a considerat că respondentul a înregistrat numele de domeniu pentru a obţine avantaje comerciale prin atragerea clienţilor săi către locaţia web a respondentului.

Respondentul a susţinut că a Maya World. S. C. a înregistrat numele de domeniu în 2002, pentru a informa, educa şi promova turismul prin Internet. Prin

---

[175] http://www.newyorktrademarkattorneyblog.com/category/domain-names/

[176] http://www.neustar.us/neustar-announces-ustld-rapid-suspension/.

[177] http://trademark-clearinghouse.com/content/tmch-stats-september-16th.

intermediul sitului său, respondentul oferă informaţii şi servicii turistice celor interesaţi de Mexic, Maya World ("Mundo Maya") şi altele. Numele de domeniu disputat utilizează două limbi (spaniolă şi engleză) şi trei cuvinte din domeniul public: COSTA (coastă), MAR (mare) şi VIAJE (călătorie), cuvinte considerate foarte populare în domeniul turismului. Aceste cuvinte sunt foarte comune şi ar trebui să poată fi folosite de oricine, contrar solicitării Costamar Travel Cruises & Tours, Inc. de folosire exclusivă şi exploatare comercială. Respondentul a susţinut că foloseşte numele de domeniu legal, fără intenţie comercială şi fără intenţia de a deturna utilizatorii Internet.

Comisia de rezolvare a disputei a considerat că marca COSTAMAR este similară de o manieră a fi confundată cu <costamartravel.com>, din moment ce cuvântul "travel" nu este suficient pentru a distinge numele de domeniu de marcă. De asemenea, a considerat că explicaţia respondentului nu demonstrează drepturi sau interese legitime în numele de domeniu. Deşi de acord că respectivele cuvinte ("costa", "mar" şi "travel") sunt foarte comune în domeniul turismului, aceasta nu înseamnă că mărcile de comerţ COSTAMAR şi COSTAMAR TRAVEL nu sunt disctincte, sau că firma Costamar Travel Cruises & Tours, Inc. nu a achiziţionat drepturi comerciale în ele (cu alte cuvinte, mărcile de comerţ COSTAMAR şi COSTAMAR TRAVEL nu sunt generice, deşi sunt formate cu termeni generici).

Respondentul are dreptul de a folosi cuvintele "costa", "mar" şi "travel", dar nu într-o manieră care să le facă similare de o manieră a fi confundate cu marca de comerţ înregistrată a Costamar Travel Cruises & Tours, Inc. Simpla intenţie de a promova turismul nu oferă drepturi sau interese legitime respondentului, din moment ce este evident că folosirea de către respondent a numelui de domeniu nu constituie folosire justă, fără scopuri comerciale. Comisia de rezolvare a disputei a concluzionat că respondent a înregistrat numele de domeniu cu rea credinţă, pentru a atrage la propria locaţie web clienţi care caută firma Costamar Travel Cruises & Tours, Inc., cu scopul de a obţine câştiguri comerciale. În acord cu paragrafele 4(i) ale *Policy* şi 15 ale *Rules*, s-a decis ca numele de domeniu <costamartravel.com> să fie transferat către Costamar Travel Cruises & Tours, Inc.

Swarovski A.G v. Modern Empire Internet Ltd (No. D2006-0148)

Swarovski A.G., Feldmeilen, Elveţia a considerat că Modern Empire Internet Ltd, din Hong Kong a înregistrat numele de domeniu <swarvoski.com> fără drept şi cu rea credinţă. Swarovski A.G. a înregistrat marca de comerţ SWAROVSKI în Hong Kong, precum şi într-o serie de alte ţări şi a considerat că numele de domeniu în dispută este similar, de natură a crea confuzie cu marca de comerţ deţinută, numele de domeniu incorporând o versiune care interschimbă literele 'o' şi 'v'. Swarovski A.G. a demonstrat că respondentul nu are drepturi sau interese legitime în numele de domeniu în dispută (căutări la registrul mărcilor de comerţ ale Hong Kong Intellectual Property Department, Singapore Intellectual Property Office, United States Patent and Trademark Office, United Kingdom Patent Office şi WIPO au arătat că repondentul nu deţine şi nu a aplicat pentru o marcă de comerţ sau de servicii a numelui de domeniu respectiv). Considerându-se că este un caz tipic de *typo-squatting* (firma care înregistrează un asemenea nume de domeniu se bazează

BCU IASI / CENTRAL UNIVERSITY LIBRARY

pe tastarea greşită a unei mărci de comerţ, implicate în numele de domeniu), în acord cu paragrafele 4(i) ale *Policy* şi 15 ale Rules, s-a luat decizia de transfer a numelui de domeniu <swarvoski.com> către Swarovski A.G.

Rolls Royce Motor Cars Limited v. Maria Stephen (No. D2006-0152)

Rolls-Royce Motor Cars Limited a reclamat-o pe Maria Stephen din SUA pentru folosirea numelor de domeniu <rollsroycepromotions.com>, <rollsroycepromotions.org> şi <rollsroycepromo.net>. Rolls-Royce Motor Cars Limited a înregistrat marca de comerţ ROLLS-ROYCE în Regatul Unit (UK) şi în SUA, în 1907 şi 1935, respectiv. În anul 2005, mesaje de poştă electronică frauduloase au fost trimise de la diferite adrese, indicând diverse nume de contact sub antetul "ROLLS ROYCE 100th ANNIVERSARY EXTRAVAGANZA" sau sub antete similare, pretinzând a fi trimise de Rolls-Royce Motor Cars Limited.

Aceste mesaje nu au fost autorizate de Rolls-Royce Motor Cars Limited, care a primit numeroase întrebări rpivind autenticitatea acestora. Mesajele de poştă electronică foloseau adrese de contact false, cum ar fi mariastephen@rollsroycepromotions.com, informau recipienţii că au câştigat 1.000.000 de lire în cadrul unei campanii promoţionale şi date personale ale recipienţilor pentru a le transfera suma, după plata unei "taxe de transfer", înşelându-i pe cei care plăteau şi expunându-i riscului de furt de identitate.

Respondentul nu avea nici un drept sau interes legitim cu privire la respectivele nume de domeniu şi nu a fost licenţiat sau autorizat de Rolls-Royce Motor Cars Limited să le folosească (nici nu a fost vorba despre folosire justă, non-comercială, legitimă a respectivelor nume de domeniu). În acord cu paragrafele 4(i) ale *Policy* şi 15 ale *Rules*, s-a decis ca numele de domeniu <rollsroycepromotions.com>, <rollsroycepromotions.org> şi <rollsroycepromo .net> să fie transferate către Rolls-Royce Motor Cars Limited.

Starwood Hotels & Resorts Worldwide, Inc. v. Domaincar (No. D2006-0136)

Starwood Hotels & Resorts Worldwide, Inc., a considerat că o serie de nume de domeniu înregistrate de respondentul Domaincar din Panama sunt asemănătoare cu mărcile sale de comerţ, lucru care stârneşte confuzie. Adiţional, unele nume de domeniu conţin posibile greşeli de tastare ale acestor mărci comerciale. Printre cele 28 de nume de domeniu disputate se numără <bangkoksheraton.com>, <bernsheraton.com>, <buenosairessheraton.com>, <chicagosheraton.com>, <fourpointssheratonhotels.com>, <hotelessheraton.com>, <manhattansheraton.com>, <neworleanssheraton.com>, <sheratonhotesl.com>, <sheratonhotls.com> etc. Starwood Hotels & Resorts Worldwide, Inc. deţine mărcile de comerţ SHERATON, WESTIN, ST REGIS şi FOUR POINTS, înregistrate la United States Patent and Trademark Office (USPTO). Starwood Hotels & Resorts Worldwide, Inc., este una dintre cele mai importante firme în domeniul hotelier, cu circa 145000 de angajaţi şi 850 de proprietăţi în circa 100 de ţari, şi investeşte sume considerabile pentru promovarea şi dezvoltarea acestor mărci prin diverse mijloace (televiziune, Internet etc.). Programul de fidelizare a clienţilor include peste 22 milioane de membri.

BCU IASI CENTRAL UNIVERSITY LIBRARY

Respondentul nu are nici un drept sau interes legitim în numele de domeniu disputate şi a fost etichetat drept *cybersquatter* în serie. Starwood Hotels & Resorts Worldwide, Inc. a dovedit că domeniile înregistrate de respondent sunt identice sau dau naştere la confuzii cu mărcile de comerţ ale sale, că respondentul nu are nici un interes legitim pentru acele nume de domenii şi că numele de domenii au fost înregistrate şi folosite cu rea credinţă. Ca urmare, s-a luat decizia de transfer a numelor de domeniu către Starwood Hotels & Resorts Worldwide, Inc.

Realtime Forex SA v. Rhone Consultants SA (No. D2006-0089)

Realtime Forex SA, Carouge, Geneva, Elveţia, a reclamat Rhone Consultants SA, Nyon, Vaud, Elveţia, în dispută fiind numele de domeniu <realtime-forex.com>. Realtime Forex SA, cu o considerabilă atenţie în media franceză şi elveţiană, activează în domeniul schimburilor de devize străine şi foloseşte platforma <www.realtimeforex.com>. Realtime Forex SA este deţinătorul mărcii de comerţ RF REALTIME FOREX, înregistrată în Elveţia în 2002. Realtime Forex SA a susţinut că traficul către domeniul disputat este redirecţionat către locaţia web a respondentului: <rcforexonline.com>. Realtime Forex SA a susţinut şi faptul că respondentul ar trebuie considerat competitor din moment ce <www.realtime-forex.com> şi <www.rcforexonline.com> oferă servicii identice: platforme pentru tranzacţii în devize străine (forex), pe aceeaşi piaţă teritorială (Elveţia) şi că numele de domeniu în cauză este similar de o manieră a fi confundat cu propria marcă RF REALTIME FOREX.

Realtime Forex SA a susţinut că respondentul nu are drepturi sau interese legitime cu privire la numele de domeniu, nefiind niciodată autorizat să folosească respectiva marcă de comerţ. Mai mult, respondentul nu a fost cunoscut sub numele folosit în domeniul în cauză, acesta fiind folosit doar pentru a redirecţiona utilizatori Internet la propria locaţie web. Numele de domeniu disputat corespunde mărcii deţinute de Realtime Forex SA, cu excepţia omisiunii literelor de prefix "rf", includerea linuţei de despărţire între cuvintele "realtime" şi "forex" şi sufixul ".com". Cele două litere "RF" corespund primei litere a cuvintelor "realtime" şi "forex" ale mărcii de comerţ, părând a fi doar o referinţă secundară sau o abreviere a mărcii. Includerea linuţei de despărţire nu afectează pronunţarea, iar ".com" este un domeniu generic de nivel înalt, ceea ce nu este suficient pentru a face un domeniu diferit sau pentru a preveni confuzia în rândul consumatorilor. Chiar dacă numele de domeniu disputat nu este pe de-a întregul identic cu marca de comerţ, modificările sunt atât de minore încât o confuzie între numele de domeniu şi marcă nu poate fi evitată.

Comisia de rezolvarea a disputei a luat în considerare că marca de comerţ RF REALTIME FOREX, sau cel puţin partea "realtime forex", folosită în numele de domeniu disputat, poate fi considerată ca generică sau descriptivă şi, prin urmare, nu poate fi folosită exclusiv. În acest caz, s-a considerat că marca de comerţ RF REALTIME FOREX serveşte ca evidenţă *prima facie* pentru validitatea mărcii de comerţ şi crează prezumpţia (discutabilă) că marca este distinctivă pentru acest tip de dispute.

Considerând că serviciile financiare oferite de respondent sub numele de domeniu disputat corespund cu serviciile oferite de Realtime Forex SA, pentru care acesta din urmă are o marcă de comerţ înregistrată, şi luând în considerare că numele de domeniu este similar de o manieră a fi confundat cu numele companiei sub care este înregistrat Realtime Forex SA, s-a considerat că este foarte probabil că numele de domeniu disputat este asociat în mintea publicului cu Realtime Forex SA şi marca de comerţ, dovedindu-se, astfel, că există riscul de confuzie. Din moment ce numele de domeniu disputat este foarte clar conectat cu numele şi marca de comerţ a Realtime Forex SA, simpla folosire de către o entitate care nu este conectată cu Realtime Forex SA sugerează rea credinţă.

Respondentul afectează afacerile Realtime Forex SA şi încearcă să atragă utilizatori Internet care intenţionează să găsească locaţia web a Realtime Forex SA prin crearea confuziei cu numele şi marca de comerţ a Realtime Forex SA. Prin urmare, Comisia a decis, în acord cu paragrafele 4(i) ale *Policy* şi 15 ale *Rules*, ca numele de domeniu în dispută să fie să fie transferat către Realtime Forex SA.

Nokia Corporation v. Nokia India Private Limited (No. D2006-0080)

Nokia Corporation, Espoo, Finlanda a solicitat transferul numelui de domeniu <nokiaind.com>, respondent fiind Nokia India Private Limited, Bangalore, Karnataka, India. Nokia Corporation, cel mai mare fabricant de telefoane mobile din lume, deţine marca de comerţ NOKIA, faimoasă în majoritatea ţărilor, situată pe poziţia a şasea în 2005 de Interbrand Corporation în topul celor mai valoroase mărci de comerţ din lume.

În acest caz, Nokia Corporation a susţinut că numele de domeniu este identic sau similar de natură a crea confuzie cu marca de comerţ NOKIA. Numele de domeniu conţine marca NOKIA şi adaugă "ind", o abreviere obişnuită pentru India. Nokia Corporation a susţinut că respondentul nu are drepturi sau interese legitime în numele de domeniu disputat. Nokia Corporation a informat Comisia de arbitraj şi mediere de faptul că nu ştie de existenţa vreunei firme numite NOKIA India PVT şi că numele de domeniu a fost înregistrat sub acest nume fals de firmă de către respondent pentru a da impresia de legitimitate.

Numele de domenii care incorporează mărci de comerţ, cazul de faţă, pot fi considerate de natură a crea confuzie cu marca de comerţ, chiar dacă se adaugă un identificator geografic la marca de comerţ. Respondentul foloseşte numele de domeniu pentru a atrage clienţi la locaţia sa web folosind misreprezentarea că locaţia web este licenţiată sau operată de Nokia Corporation. Un distribuitor poate face *bona fide* oferte de bunuri sau servicii, având, astfel, un interes legitim în numele de domeniu dacă folosirea respectă următoarele cerinţe:

(1) Respondentul oferă bunurile sau serviciile în cauză;
(2) Respondentul foloseşte locaţia pentru a vinde doar bunuri cu marca respectivă; şi
(3) Locaţia web descrie corect relaţia registrantului cu deţinătorul mărcii de comerţ.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

În acest caz, respondentul nu îndeplinea toate aceste cerințe, în consecință, în acord cu paragraful 4(i) al *Policy* și paragraful 15 al *Rules*, Comisia a decis ca numele de domeniu <nokiaind.com> să fie transferat către Nokia Corporation.

Banca di Roma S.p.A. v. Unasi Inc. a/k/a Domaincar (No. D2006-0068)

Banca di Roma S.p.A., Roma, Italia, a disputat numele de domeniu <bancadiroma.net>, repondent fiind Unasi Inc. a/k/a Domaincar, Panama. Banca di Roma S.p.A., fondată în 1992, este o bancă importantă, cu 12 locații principale în Italia și un număr de sucursale în lume. Banca di Roma S.p.A. deține un număr de mărci de comerț care incorporează cuvintele "Banca di Roma".

Banca di Roma S.p.A. a argumentat că respondent nu are drepturi sau interese legitime în numele de domeniu disputat, că acesta nu a demonstrat *bona fide* că oferă bunuri sau servicii înainte de startul procedurii și că numele de domeniu disputat a fost înregistrat și folosit cu rea credință, urmărind doar inducerea în eroare a clienților care, datorită redirectării pe web, pot crede că serviciile bancare oferite sunt legate de cele oferite de Banca di Roma S.p.A. Banca di Roma S.p.A. a explicat că această situație are un dublu efect negativ: (i) respondentul beneficiază de pe urma faimei mărcii de comerț și (ii) serviciile financiare oferite prin intermediul portalului accesibil via numele de domeniu în dispută nu sunt la același standard de calitate, ceea ce este de natură să prejudicieze Banca di Roma S.p.A.

Respondentul nu a furnizat nici un element sau circumstanță care să justifice drepturi sau interese legitime, conform paragrafului 4(c) al *Policy*, sau că ar fi cunoscut după numele de domeniu în dispută. Comisia de arbitraj și mediere a concluzionat că marca de comerț BANCA DI ROMA este unică și bine cunoscută în Italia și câteva alte țări și că nu este probabil ca respondentul să fi înregistrat sau folosit acest nume de domeniu fără a fi conștient de marca de comerț, prin urmare folosindu-l cu rea credință: pentru a deturna utilizatori Internet care caută informații despre produsele Banca di Roma. Mai mult, respondentul a fost implicat în cel puțin 30 de alte cazuri UDRP, toate terminându-se cu transferul numelor de domeniu în dispută către reclamant.

Luând în considerare aceste aspecte, Comisia de arbitraj și mediere a considerat că respondentul este prolific în înregistrarea de nume de domenii prolific cu obiectivul de a împiedica deținători de mărci de comerț de a reflecta mărcile respective în nume de domeniu corespunzătoare. Pentru toate aceste motive, în acord cu paragrafele 4(b)(ii and iv) ale *Policy* și 15 ale *Rules*, Comisia a dispus transferul numelui de domeniu <bancadiroma.net> către Banca di Roma S.p.A.

WeddingChannel.com, Inc. v. Helois Lab (No. D2006-0021)

WeddingChannel.com, Inc., Los Angeles, California, SUA a disputat numele de domeniu <macys-weddingchannel.com>, respondent fiind Helois Lab, Eldoret, Kenya. WeddingChannel.com, Inc. deține mai multe mărci de comerț care constau sau includ cuvintele "Wedding Channel" pentru un domeniu larg de servicii legate de sau incidentale aranjamentelor de nuntă, consultanță, informații de călătorie etc. WeddingChannel.com, Inc. este, de asemenea, deținătorul numelui de domeniu <weddingchannel.com>, care conține legături *hypertext* la un număr

BCU IASI / CENTRAL UNIVERSITY LIBRARY

de magazine de tip *retail* din SUA, cum ar fi JC Penney, Tiffany & Co., Bloomingdale's ş.a., şi, prin înţelegere cu deţinătorul mărcii de comerţ MACY'S, deţinătorul numelui de domeniu <macysweddingchannel.com>. WeddingChannel .com, Inc. a susţinut în acest caz că respondentul, sub o varietate de alias-uri, are o lungă istorie de nume de domenii înregistrate în legătură cu mărci de comerţ care au fost subiect al mai multor decizii UDRP adverse.

Comisia a considerat că respondentul nu are drepturi sau interese legitime, numele de domeniu fiind înregistrat cu rea credinţă, cu intenţia de a atrage clienţi la acea locaţie web pentru câştiguri comerciale prin crearea posibilităţii de confuzie cu WeddingChannel.com, Inc. şi marcile sale de comerţ. De asemenea, respondentul a manifestat intenţia de a vinde numele de domeniu pentru profit. Comisia de arbitraj şi mediere a considerat că numele de domeniu este similar de o manieră a fi confundat cu marca de comerţ sau servicii în care WeddingChannel.com, Inc. are drepturi. Numele de domeniu în dispută nu are nici o asemănare cu numele după care respondentul este cunoscut, folosirea numelui de domeniu fiind clar comercială, cu intenţia de a misdirecţiona consumatori către locaţii web care sunt competitori direcţi ai WeddingChannel.com, Inc. şi ai clienţilor săi. În acord cu paragrafele 4(i) ale *Policy* şi 15 ale *Rules*, Comisia a dispus transferul numelui de domeniu <macys-weddingchannel.com> să fie transferat către WeddingChannel.com, Inc.

Wal-Mart Stores, Inc. v. Terry Davies (No. D2006-0031)

Wal-Mart Stores, Inc., Arizona, SUA a disputat numele de domeniu <wal-mart-superstore.com>, respondent fiind Terry Davies, Calgary, Canada. Wal-Mart Stores, Inc., cel mai mare *retailer* din lume, având peste 1300 magazine şi peste 1700 supercentre, foloseşte extensiv Internetul pentru a-şi desfăşura activitatea, operând locaţii web cum ar fi <www.walmart.com>, <www.wal-mart.com>, <www.walmartstores.com>, <www.walmartsuperstore.com> etc. Wal-Mart Stores, Inc. deţine numeroase mărci de comerţ, inclusiv WAL-MART. Wal-Mart Stores, Inc. a susţinut că numele de domeniu în dispută este similar de o manieră a fi confundat cu marca WAL-MART, argumentând că termeni adiţionali într-un nume de domeniu neschimbând această percepţie, mai ales când sunt de natură nedistinctivă, fiind înregistrat cu rea credinţă.

Comisia de arbitraj şi mediere a concluzionat că numele de domeniu disputat este similar de o manieră a fi confundat cu marca în care Wal-Mart Stores, Inc. are drepturi, fiind folosit fără drept sau interes legitim şi cu rea credinţă, conform paragrafelor 4(a) (iii) şi 4(b)(iv) ale *Policy*. Pentru aceste motive, în acord cu paragrafele 4 ale *Policy* şi 15 ale *Rules*, Comisia a dispus transferul numelui de domeniu <wal-mart-superstore.com> către Wal-Mart Stores, Inc.

Six Continents Hotels, Inc. v. Tripod UK Ltd (No. D2006-0041)

Six Continents Hotels, Inc., InterContinents Hotels Group, Atlanta, Georgia, SUA, a disputat numele de domeniu <crownplaza.net>, respondent fiind Tripod UK Ltd, Fulham, Londra, Regatul Unit (UK). Six Continents Hotels, Inc., direct sau prin afilieri, deţine, administrează sau oferă francize pentru suita de

BCU IASI / CENTRAL UNIVERSITY LIBRARY

hoteluri CROWNE PLAZA, HOLIDAY INN, HOLIDAY INN EXPRESS, HOLIDAY INN SELECT etc. Six Continents Hotels, Inc. a demonstrat drepturile sale în familia de mrci de comerţ CROWNE PLAZA şi a furnizat informaţii privind prezenţa sa pe Internet, prin înregistrarea şi operarea numelor de domeniu <crowneplaza.com> şi <crownplaza.com> (cu evidenţierea lipsei literei "e" în ultimul nume de domeniu). Considerând că numele de domeniu disputat este aproape identic cu mărcile de comerţ înregistrate ale Six Continents Hotels, Inc., confuzia cu numele de domeniu al respondentului este evidentă.

Absenţa literei "e" nu afectează pronunţarea mărcii de comerţ. Lipsa literei "e" este o greşală de tastare frecventă care nu schimbă esenţa mărcii de comerţ pentru a permite o distincţie clară între această marcă şi numele de domeniu în cauză. Numele de domeniu disputat evocă imediat hotelurile CROWNE PLAZA, sugerând o relaţie care nu există între Six Continents Hotels, Inc. şi respondent. Mai mult, numele de domeniu găzduieşte legături către alte locaţii web de hoteluri, ceea ce contribuie la confuzionarea utilizatorilor Internet.

Comisia de arbitraj şi mediere a considerat că numele de domeniu este esenţial identic şi similar de o manieră a fi confundat cu mărcile înregistrate ale Six Continents Hotels, Inc., satisfăcând cerinţele paragrafului 4(a) (i) al *Policy*. Respondentul nu a demonstrat nici un drept sau interes legitim în numele de domeniu <crownplaza.net>, nici nu a prezentat argumente care să demonstreze că este cunoscut după acest nume de domeniu. Considerând similaritatea între numele de domeniu şi marca de comerţ CROWNE PLAZA, s-a considerat că respondentul foloseşte numele de domeniu în încercarea de a îl vinde, profitând de valoarea mărcii şi, pe de altă parte, pentru a atrage utilizatori Internet la locaţii web ale competitorilor, ceea ce, evident, nu constituie folosire *bona fide*.

Datorită reputaţiei de care se bucură marca de comerţ CROWNE PLAZA, respondentul evidenţiază reaua credinţă prin oferirea numelui de domeniu pentru vânzare, considerând că preţul vânzării sale va reflecta faima mărcii de comerţ. Pentru aceste motive, în acord cu paragrafele 4 ale *Policy* şi 15 ale *Rules*, Comisia a dispus transferul numelui de domeniu <crownplaza.net> către Six Continents Hotels, Inc.

2.12.2 Cazuri privind numele personale

Numele personale faimoase sunt adesea folosite în mod abuziv în numele de domenii Internet[178]. De-a lungul timpului, astfel de cazuri au implicat artişti pop (spre exemplu, *Madonna Ciccone, p/k/a Madonna v. Dan Parisi and 'Maddona.com'*, WIPO Case No. D2000-0847); actori (spre exemplu, *Isabelle Adjani v. Second Orbit*, WIPO Case No. D2000-0867); sportivi (spre exemplu, *Serena Williams and Venus Williams v. Eileen White Byrne and Allgolfconsultancy*, WIPO Case No. D2000-1673); politicieni (*The Honorable Ron Paul v. DN Capital Inc., Martha Roberts*, WIPO Case No. D2013-0371) etc.

[178] Vezi I. Vasiu, L. Vasiu, *Folosirea numelor personale în numele de domeniu Internet*, Revista Română de Dreptul Proprietăţii Intelectuale, IV, 2 (11), 47-57, 2007.

Numele personale care au fost înregistrate ca mărci sunt protejate conform UDRP. După cum explică WIPO[179], chiar dacă UDRP nu protejează în mod expres numele de persoane ca atare, în situațiile în care un nume de persoană neînregistrat ca o marcă este utilizat pentru comerț, reclamantul poate fi în măsură să stabilească drepturi de marcă neînregistrată în acel nume. Pentru a face acest lucru, trebuie dovedită utilizarea numelui persoanei ca un identificator distinctiv de bunuri sau servicii, oferite sub acest nume.

O bază echivalentă cu marca se consideră că există în acțiunea *common law* numită *passing-off*, care are, în general, are scopul de a preveni efectuarea de interpretări greșite ale publicului în contextul comerțului și care, dacă a fost stabilită, poate constitui motiv pentru recurgerea la un nume personal în scopul UDRP. Cu toate acestea, numele în cauză trebuie să fie utilizat efectiv în comerț, ca un identificator de bunuri sau servicii pentru a stabili drepturile de marcă neînregistrate în scopul UDRP. Simpla existență a unui nume celebru sau includerea de afirmații nesusținute de fapte cu privire la utilizarea respectivului nume în comerț nu sunt, în mod normal, suficiente pentru a demonstra drepturile de marcă neînregistrate.

Pamela Anderson v. Alberta Hot Rods (No. D2010-1144)

În acest caz, numele de domeniu disputat a fost <pamanderson.com>. Reclamanta este deținătorea a numeroase mărci pentru PAMELA ANDERSON, care acoperă numeroase bunuri și servicii. Reclamanta a susținut că numele său servește ca marcă, bazată pe faima sa mondială ca actrița, ea fiind cunoscută profesional ca "Pam Anderson". În plângere s-a precizat că înregistrarea acestui nume de domeniu este realizată cu rea-credință, fiind o încercare clară de a obține avantaje de pe urma faimei sale și că respondentul nu are drepturi sau interese legitime în acest nume de domeniu, acesta nefiind, ca persoana fizică sau juridică, cunoscut sub numele de "Pam Anderson".

Respondentul a argumentat că numele "Pam Anderson" și numele de domeniu disputat nu sunt identice cu numele real al reclamantei, Pamela Denise Anderson; adițional, toate mărcile reclamantei sunt înregistrate ca "PAMELA ANDERSON", nu "PAM ANDERSON", neexistând o confuzie între numele de domeniu disputat și numele reclamantei. Mai mult, reclamanta nu a demonstrat că majoritatea căutărilor după "Pam Anderson" conduc către <pamanderson.com> și că nu ar exista confuzie bazată pe acest nume de domeniu. Respondentul a argumentat că înregistrarea de mărci diferite de numele său real demonstrează încercarea de a acoperi cât mai mult "teritoriu" și a securiza cât mai multe nume de domeniu, abuzând, astfel, procesul UDRP.

Comisia a considerat că "Pam" este o abreviere comună a numelui "Pamela", publicul putând prezuma că "Pam Anderson" reprezintă reclamanta și că numele de domeniu este similar cu drepturile reclamanta, în măsură să producă confuzie, satisfăcând solicitarea paragrafului 4(a)(i) al *Policy*. Comisia a concluzionat și că reclamanta a demonstrat că respondentul nu are drepturi sau

[179] Vezi http://www.wipo.int/amc/en/domains/search/overview2.0/#16.

interese legitme cu privire la numele de domeniu disputat, conform paragrafelor 4(a)(ii) şi 4(c) ale *Policy*. Considerând că respondentul a înregistrat cu rea-credinţă numele de domeniu, în acord cu paragrafele 4(i) ale *Policy* şi 15 ale *Rules*, Comisia de arbitraj a ordonat transferul numelui de domeniu <pamanderson.com> către reclamantă.

2.12.3 Cazuri privind indicațiile geografice

Protecţia indicaţiilor geografice ridică probleme semnificative în raport cu folosirea acestora în cadrul numelor de domeniu Internet. Astfel, Raportul final al *Second WIPO Internet Domain Name Process*[180] evidenţiază folosirea abuzivă a indicaţiilor geografice în numele de domeniu Internet. Printre numele de domeniu Internet există unele înregistrate fără a avea nici o conexiune cu indicaţia geografică implicată, fapt care induce în eroare utilizatorii şi consituie piraterie comercială. Exemple în acest sens pot fi considerate <bourgogne.com>, <cotnari.com>, <ouzo.com>, <montepulciano.com>, <medoc.com>, <champagne.org>, <cognac.net>, <chianti.com>, <chateauneuf-du-pape.com>, <sangiovese.com>, <tequila.com>, <xeres.com> etc.[181] Dacă un nume de domeniu înregistrat este o indicaţie geografică şi este fals sau induce în eroare, se poate considera o violare a interdicţiei de a folosi indicaţii false, stipulată în Art. 3bis al *Madrid Agreement* sau în *TRIPS Agreement*[182].

Comité Interprofessionnel du vin de Champagne v. Steven Vickers
(Case No. DCO2011-0026)

Numele de domeniu în acest caz a fost <champagne.co>. Reclamantul a argumentat că vânzările de vin sub numele "Champagne" au fost substanţiale, atât în ceea ce priveşte volumul, cât şi valoarea acestora, numele "Champagne" având o valoroasă reputaţie globală. Conform plângerii, expresia "champagne" nu a devenit numele comun al unui vin în UE, fiind distinctiv numai pentru vinul produs în regiunea Champagne din Franţa. Folosirea cuvântului "champagne" este reglementată în toată UE ca o "denumire de origine", conform Regulation (EC) No. 491/2009. Reclamantul deţine 27 gTLDs şi ccTLDs care constau din cuvântul "champagne" şi alte 101 nume de domeniu care includ cuvântul "champagne" ca parte a numelui. Aceste nume de domeniu includ <champagne.eu>, <champagne.biz>, <champagne.com>, <champagne.fr>, <champagne.co.uk> etc.

Respondentul a arătat că, în dicţionare online, cuvântul "champagne" apare scris cu "C", ca referinţă la regiunea Champagne, dar şi scris cu "c", cu referinţă la

---

180 A se vedea Standing Committee on the Law of Trademarks, Industrial Designs and Geographical Indications, *Internet domain names and geographical indications*, Geneva (2003).

181 Vezi WIPO, *Internet Domain Names and Geographical Indications*, 2003, disponibil la locaţia www.wipo.int/edocs/mdocs/sct/en/sct_10/sct_10_6.doc.

182 De remarcat, în acest context, aspectele jurisdicţionale (spre exemplu, în situaţia în care o indicaţie geografică este recunoscută într-o ţară, dar considerată generică şi descriptivă conform legilor altei ţări).

vinul spumos. Respondentul a aratat şi că o căutare Google după cuvântul "champagne" a produs 19 milioane de rezultate pe site-uri din United Kingdom, el considerând că "champagne" este un tip de vin spumos. Adiţional, respondentul a argumentat că faptul că reclamantul deţine numeroase nume de domeniu "champagne" nu demonstrează, în sine, că a obţinut drepturi de marcă privind termenul "champagne".

Comisia a considerat că reclamantul nu a demonstrat că expresia "Champagne" constituie o marcă neînregistrată, conform cerinţei paragrafului 4(a)(i) al *Policy*. Comisia a remarcat că, pentru a fi o marcă, un semn trebuie să poată distinge bunurile sau serviciile unei entităţ de cele ale alteia şi a considerat că o indicaţie geografică *per se* nu permite distincţia între vinul unui producător *champagne* de al altuia, neîndeplinind, aşadar, funcţia fundamentală a unei mărci de a permite distincţia între bunuri şi servicii, conform Art. 2 al Directivei privind mărcile (Directiva 2008/95/EC). O indicaţie geografică este, în mod esenţial, desemnată să protejeze producătorii dintr-o anumită regiune de pierderi cauzate de aplicarea fără drept a acelui identificator pe bunuri care nu au fost produse în acea regiune, indicaţiile geografice indicând fundamental calitatea şi reputaţia bunurilor produse, în acord cu anumite standarde, într-o arie geografică specifică, dar nu despre o anumită sursă individuală ca atare. Comisia a mai argumentat şi că nu consideră că *Policy* a intenţionat ca indicaţiile geografice sau "denumirile de origine protejate" trebuie să consituie o bază pentru un asemenea "drept" conform paragrafului 4(a)(i), refunzând plângerea.

2.12.4 Cazuri privind numele internaţionale non-proprietar pentru substanţele farmaceutice

Numărul mare de preparate proprietare conţinând o anumită substanţă poate genera confuzie în privinţa identificării unui ingredient activ. Existenţa unui sistem nomenclator pentru numele internaţionale non-proprietar (NIN) pentru substanţele farmaceutice[183] este crucială pentru identificarea clară, prescrierea sau furnizarea de medicamente şi pentru comunicarea şi schimbul de informaţii între persoanele din acest domeniu. Un nume internaţional non-proprietar (*International Nonproprietary Name - INN*, cunoscut şi ca *rINN*, de la *recommended International Nonproprietary Name*) este numele care nu aparţine unei persoane (non-proprietar), nume generic dat unei substanţe farmaceutice, desemnat de Organizaţia Mondială a Sănătăţii (*World Health Organization* - WHO), nume unic, global recunoscut, proprietate publică.

[183] Spre exemplu, *ampicillin, ibuprofen, sildenafenil* etc. Pentru o listă INN vezi World Health Organization, *International Nonproprietary Names (INN) for pharmaceutical substances Names for radicals & groups comprehensive list*, Geneva, 2004; World Health Organization, *WHO Drug Information*, Vol. 17, No. 2, 2003. Vezi http://www.who.int/medicines/services/inn/en/.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

Sistemul NIN facilitează comunicarea prin furnizarea unui nume standard pentru fiecare substanţă[184]. Organizaţia Mondială a Sănătăţii are responsabilitatea dezvoltării şi promovării de standarde internaţionale în acest domeniu. Sistemul NIN a fost iniţiat în anul 1950 de către Rezoluţia WHA3.11 a World Health Assembly şi a devenit operaţional în anul 1953, când a fost publicată o listă iniţială de nume internaţionale non-proprietar pentru substanţele farmaceutice. Actualmente, lista cuprinde circa 7.000 de nume, numărul acestora crescând cu circa 120-150 anual[185]. Numele de pe această listă sunt selectate în colaborare cu comisii naţionale, cum ar fi SUA (*United States Adopted Name*), Italia (*Denominazione Comune Italiana*), Franţa (*Dénomination Commune Française*), Japonia etc. Situaţiile în care un nume generic naţional pentru o nouă substanţă farmaceutică diferă de NIN sunt foarte rare[186].

O solicitare de selectare pentru lista NIN este trimisă Organizaţiei Mondiale a Sănătăţii, de regulă prin intermediul autorităţii naţionale de nomenclatură, conţinând informaţii precise asupra chimiei, acţiunii şi folosirii farmacologice, numele propus, numele şi adresa fabricantului. Fiecare nume propus este examinat, toţi membrii comisiei de experţi a Organizaţiei Mondiale a Sănătăţii privind *International Pharmacopoeia and Pharmaceutical Preparations* desemnaţi să selecteze nume generice trebuie să accepte numele, care este apoi publicat ca *NIN propus*[187]. Timp de patru luni, orice persoană poate obiecta asupra numelui propus, pe motiv de similaritate cu nume de comerţ.

Dacă nu sunt ridicate obiecţii, numele propus este publicat ca *NIN recomandat*[188]. Principalele principii[189] pentru selectare unui nume pentru lista NIN sunt distinctivitatea în sunet şi silabisire; lungimea rezonabilă; şi improbabilitatea confuziei cu alte nume în folosinţă curentă. Două liste de NIN propuse şi două liste de NIN recomandate sunt publicate anual în mai multe limbi (engleză, franceză, spaniolă, latină).

Înregistrarea NIN ca nume de domeniu Internet

Organizaţia Mondială a Sănătăţii a abordat Organizaţia Mondială a Proprietăţii Intelectuale (WIPO) pentru a explora modalităţi de cooperare care să asigure protejarea NIN împotriva folosirii abuzive şi însuşirii prin înregistrare ca

---

184 Vezi definiţia de la http://www.wikipedia.com.

185 Vezi *Guidance on INN* la locaţia http://www.who.int/medicines/services/inn/innguidance/en/.

186 Vezi World Health Organization, *International Nonproprietary Names (INN) for pharmaceutical substances Names for radicals & groups comprehensive list*, Geneva, 2004.

187 Procedura curentă pentru selectarea INN recomandat a fost adoptată de Executive Board în 1955 în rezoluţia EB15.R7, amendată de rezoluţia EB43.R9, adoptată în 1969.

188 Numele selectate sunt publicate în periodice ale Organizaţiei Mondiale a Sănătăţii (*WHO Drug Information*). Pentru acces web s-a creat o bază de date la locaţia http://www.who.int /druginformation/general/innlists.shtml.

189 Vezi World Health Organization, *International Nonproprietary Names (INN) for pharmaceutical substances Names for radicals & groups comprehensive list*, 2004; *Guidelines on the Use of International Nonproprietary Names (INNs) for Pharmaceutical Substances* (WHO/PHARM S/NOM 1570); World Health Organization, Executive Board EB110/3, *International Nonproprietary Names: revised procedure*, Report by the Secretariat, 2002.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

mărci de comerț[190]. Subiectul NIN a fost pe agenda primei întâlniri a Comitetului privind dreptul mărcilor, design-ului industrial și indicațiilor geografice, în 1998[191].

Principala sursă de conflict este, de regulă, încercarea unor entități de a propune o nouă marcă de comerț care conține elemente ale unui cuvânt din sistemul NIN pentru a demonstra relația între substanțe farmacologice. Pentru a preveni conflictul între NIN și mărcile de comerț, a fost adoptată rezoluția WHA46.19 în 1993, care solicită statelor membre ale Organizației Mondiale a Sănătății să dezvolte politici de folosire și protejare a NIN și să descurajeze folosirea ca mărci de comerț a numelor comerciale derivate NIN[192].

La cea de-a XV-a sesiune a SCT, care a avut loc la sfârșitul anului 2005, s-a solicitat Organizației Mondiale a Proprietății Intelectuale să aibă consultări cu Organizația Mondială a Sănătății asupra modurilor de popularizare a informațiilor asupra NIN statelor membre[193]. La o sesiune specială WIPO[194], s-a exprimat punctul de vedere că NIN sunt termeni generici, deci, prin definiție, nu pot fi subiectul unui abuz. Orice înregistrare a unui nume de domeniu crează o exclusivitate *de facto* în numele de domeniu, prin urmare, în cazul termenilor generici, nu pot fi aduse argumente persuasive în favoarea stabilirii unei protecții care se bazează pe o asemenea exclusivitate. Reprezentantul EFPIA (European Federation of Pharmaceutical Industries and Associations)[195] s-a pronunțat în favoarea unui mecanism de excludere/blocare pentru înregistrarea oricărui nume de domeniu identic cu un NIN, mecanism care ar trebui aplicat tuturor înregistrărilor, din trecut sau viitor. Printre alte puncte de vedere exprimate, s-a evidențiat cel care a susținut că situațiile în care o locație web asociată cu un NIN conține informații frauduloase pot fi abordate prin prisma legislației naționale din domeniu și a evidențiat necesitatea furnizării de dovezi privind daunele cauzate de asemenea înregistrări.

Teva Pharmaceutical Industries Limited v. BLTC Research
(Case No. D2005-0113)

În acest caz, Teva Pharmaceutical Industries Limited a fost reclamant, BLTC Research reclamat, numele de domeniu disputat fiind <rasagiline.com>.

---

190 Vezi WIPO, *International nonproprietary names for pharmaceutical substances*, Standing committee on the Law of Trademarks, Industrial designs and Geographical indications, Third Session, Geneva, (1999); WIPO Publication No. 439(E), *Report of the WIPO Internet Domain Name Process*, paragrafele 296-303.

191 Vezi *Final Report of the WIPO Internet Domain Name Process*, 1999.

192 Vezi *Guidelines on the Use of International Nonproprietary Names (INNs) for Pharmaceutical Substances* la http://whqlibdoc.who.int/hq/1997/WHO_PHARM_S_NOM_1570.pdf.

193 Vezi WIPO, *Marks and international nonproprietary names for pharmaceutical substances (INNs)*, Standing Committee on the Law of Trademarks, Industrial designs and Geographical indications, Sixteenth Session, Geneva, 2006.

194 Vezi WIPO Standing Committee on the Law of Trademarks, Industrial designs and Geographical indications, *Second Special Session on the Report of the Second WIPO Internet Domain Name Process*, Report adopted by the Special Session of the Standing Committee, Geneva, 2002.

195 Voce reprezentativă a industriei farmaceutice în Europa, reprezentând punctele de vedere și interesele a peste 3350 companii implicate în cercetarea și fabricarea de produse medicinale.

BCU IASI CENTRAL UNIVERSITY LIBRARY

Reclamantul a dezvoltat un nou medicament, care a primit în anul 1994 NIN *rasagiline*. Medicamentul este protejat prin patent în mai multe ţări. În 2004, reclamantul a dorit să achiziţioneze numele de domeniu de la reclamat pentru suma de $4.000, dar oferta nu a fost acceptată, reclamatul dorind o sumă mult mai mare. Chiar dacă reclamantul acceptă că *rasagiline* este un NIN, prin urmare nu poate fi înregistrat ca marcă de comerţ, Teva este singura entitate care controlează vânzarea de produce care conţin *rasagiline* şi singura prin care *rasagiline* este furnizat; prin urmare reclamantul considera că este exclusiv asociat cu *rasagiline*, aceasta trebuind considerată ca o marcă neînregistrată în care are drepturi substanţiale.

În caz s-a argumentat că reclamatul nu are nici un interes legitim în numele de domeniu în dispută, acesta, sub masca furnizării de informaţii către public, făcând, de fapt, o înregistrare cu rea credinţă (cazul de faţă nefiind singurul în care reclamatul a incorporat NIN în nume de domeniu înregistrate), urmărind împiedicarea companiilor îndreptăţite să folosească numele respective. Reclamatul a răspuns că NIN se află în domeniul public şi nu pot fi arbitrate conform UDRP, <rasagiline.com> nu este identic sau similar de natură a crea confuzie cu o marcă înregistrată a reclamantului [cerinţă expresă a paragrafului 4(a) al UDRP]. Comisia de arbitraj a decis că reclamantul nu are o marcă de comerţ înregistrată în înţelesul paragrafului 4(a) al UDRP şi a respins solicitarea reclamantului.

Biofarma v. UltimateDomains.com/Jarred Cohen (Case No. D2005-0979)

În acest caz reclamant a fost Biofarma, reclamat UltimateDomains.com /Jarred Cohen, printre domeniile în dispută aflându-se <genericgliclazide.com>, <gliclazide.org> şi <gliclazide.net>. Reclamantul este deţinătorul mărcii înregistrate DIAMICRON şi producătorul produsului farmaceutic care a primit NIN *gliclazide*. Reclamatul a oferit la vânzarea prin licitaţie numele de domeniu în dispută.

Reclamatul, făcând referire la paragraful 4(a)(i) al UDRP, a argumentat că folosirea de termeni generici nu afectează mărci înregistrate, iar cu referire la celelalte cerinţe ale UDRP a susţinut că situaţiile descrise nu sunt aplicabile în acest caz. Referitor la paragraful 4(a)(i) al UDRP, reclamantul a argumentat că numele în dispută <gliclazide.net>, <gliclazide.org> şi <genericgliclazide.net> sunt identice cu NIN *gliclazide*, reclamatul nefiind cunoscut sub acest nume şi nici nu vinde produse cu acest nume, neavând nici un interes non-comercial în folosirea numelor de domeniu <gliclazide.net>, <gliclazide.org> şi <genericgliclazide.net>, aceste nume de domeniu fiind înregistrate cu scopul principal de a fi vândute reclamantului pentru o sumă mult mai mare decât costurile directe.

Comisia de arbitraj a analizat dacă un NIN poate fi considerat marcă de comerţ în înţelesul paragrafului 4(a)(i) al UDRP, considerând că nu este cazul, prin urmare nu a mai luat în discuţia reaua credinţă sau inexistenţa unor interese legitime în folosirea numelor de domeniu <gliclazide.net>, <gliclazide.org> şi <genericgliclazide.net>. Solicitarea anulării numelor de domeniu menţionate a fost respinsă.

3. DREPTURI DE PROPRIETATE INTELECTUALĂ ÎN CYBERSPAȚIU

Drepturile de proprietate intelectuală pot fi divizate în două categorii principale[196]:

(i) Drept de autor și drepturi conexe;

(ii) Drepturi de proprietate industrială, care, la rândul lor, pot fi împărțite în *protecția semnelor distinctive* (mărci și indicații geografice) și *pentru stimularea inovației și crearea de tehnologii* (brevete de invenție, design industrial și secrete comerciale).

Conform Art. 7 al Acordului TRIPS (*Trade-related aspects of intellectual property rights*), protecția drepturilor de proprietate intelectuală trebuie să contribuie la promovarea innovației tehnologice și la transferul sau diseminarea tehnologiei, în avantajul mutual al producătorilor și utilizatorilor, de o manieră care să favorizeze bunăstarea socială și economică și să echilibreze drepturi și obligații. Protecția acestor drepturi a devenit dificilă, mijloacele digitale deschizând noi căi de încălcare a drepturilor de autor[197], atacurile putând fi realizate teoretic din interiorul unei organizații[198] sau din orice locație exterioară organizației, cu posibilitatea reală ca infractorii să nu fie depistați.

Încălcarea drepturilor de proprietate intelectuală reprezintă un fenomen îngrijorător prin dimensiunile sale, prin potențialul de a cauza pierderi masive titularilor drepturilor și economiilor naționale și prin problemele pe care le ridică privind protecția consumatorilor. Potrivit unui studiu, firmele pierd circa un trilion de dolari anual datorită încălcării drepturilor de proprietate intelectuală[199]. Printre cele mai lucrative activități infracționale împotriva drepturilor de proprietate intelectuală se numără obținerea secretelor comerciale[200].

---

[196] Vezi *What are intellectual property rights?*, http://www.wto.org/english/tratop_e/trips_e/intel1_e.htm.

[197] Conform Legii nr. 8/1996, art. 140 1 (c) comunicarea publică a operelor sau produselor purtătoare de drepturi conexe fără autorizarea sau consimțământul titularilor constituie infracțiune - vezi o analiză a infracțiunii în C. R. Romițan, *Infracțiunea de comunicare publică a operelor sau produselor purtătoare de drepturi conexe*, Revista Română de Dreptul Proprietății Intelectuale, III, 2 (7), 54-67, 2006; M. B. Bulancea, *Infracțiunea de punere la dispoziția publicului, fără consimțământul titularilor de drepturi, a produselor purtătoare de drepturi de autor, de drepturi conexe sau de drepturi sui-generis ale fabricanților de baze de date*, Revista Română de Dreptul Proprietății Intelectuale, III, 4 (9), 67-80, 2006. Vezi și S. W. Brenner, Is There Such a Thing as "Virtual Crime"?, 4 California Criminal Law Review 1, 2001; J. T. Wells, Enemies Within: Asset misappropriation comes in many forms, 2001.

[198] Vezi M. R. Randazzo, D. Cappelli, M. Keeney, A. Moore, E. Kowalski, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, United States Secret Service and Carnegie Mellon University, 2004.

[199] Vezi JP Morgan Chase, *Cybercrime: The Growing Global Threat*, 2011.

[200] Vezi Ioana Vasiu și Lucian Vasiu, *Protecția secretelor comerciale în domeniul tehnologiei informației*, Revista Română de Dreptul Proprietății Intelectuale, VII, 4 (25), 71–79, 2010;

Adesea, făptuitorii sunt persoane din interior, foşti sau actuali angajaţi, contractori sau parteneri de afaceri care, cu intenţie, depăşesc sau folosesc în interes personal autorizarea de acces la date sau sisteme informatice pentru a obţine secrete comerciale aparţinând organizaţiei victimă; conform unui studiu[201], în peste 85% dintre cazurile de furt de secrete comerciale făptuitorul a fost o persoană care era fie angajat, fie partener de afaceri al deţinătorului secretului comercial. Mai mult, acest fenomen pare a fi din ce în ce mai legat de crima organizată[202].

Încălcarea drepturilor de autor se petrece adesea prin achiziţionare sau folosire neautorizată şi poate afecta categorii largi de lucrări protejabile (*inter alia*): lucrări literare (cărţi, articole, programe informatice, compilaţii de informaţii, baze de date) lucrări muzicale, înregistrări audio, filme etc.). Un mediu deosebit de favorabil încălcării drepturilor de proprietate intelectuală este reprezentat de site-urile cu continut generat de utilizatori (UGC)[203].

Contrafacerea comercială[204], pe de altă parte, este una dintre formele cele mai periculoase de încălcare a drepturilor de proprietate intelectuală[205] şi a devenit o ameninţare majoră la adresa economiei mondiale, prin creşterea sa exponenţială şi prin dimensiunile sale globale. Astfel, dacă în 1982 se estima că fenomenul implică sume de circa 5,5 miliarde dolari, în 1996 cifra era estimată la 200 miliarde dolari, iar în 2003 la circa 400-500 miliarde dolari[206]. Unele estimări consideră că acest

---

Jason Mazzone şi Matthew Moore, *The Secret Life of Patents*, Washburn Law Journal, Vol. 48, 2008.

201 Vezi David S. Almeling şi colab., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, Gonzaga Law Review, Vol. 45, 2010.

202 Vezi Commission of the European Communities, *Amended proposal for a Directive of the European Parliament and of the Council on criminal measures aimed at ensuring the enforcement of intellectual property rights*, Brussels, 2006.

203 Vezi Ioana Vasiu şi Lucian Vasiu, *We Create, You Tube, They Infringe: Cases and Considerations Regarding Intellectual Property Rights on User Generated Content Websites*, Revista Română de Dreptul Proprietăţii Intelectuale, 3, 95-103, 2013.

204 Conform Council Regulation (EC) Nr. 1383/2003, Art. 2 (1) (a) prin "bunuri contrafăcute" se înţelege:
(i) bunuri, incluzând modul de ambalare, care poartă fără autorizare o marcă comercială identică unei mărci înregistrate valid pentru acelaşi tip de bunuri sau care nu poate fi distinsă în aspectele ei esenţiale de o asemenea marcă, încălcând astfel drepturile titularului conform dreptului comunitar, aşa cum este stipulat în Council Regulation (EC) No 40/94 din 20 Decembrie 1993 sau de dreptul statului membru în care aplicaţia pentru acţiune a autorităţilor vamale este realizată;
(ii) orice simbol de marcă (incluzând logo, etichetă, broşură, instrucţiuni de folosire sau document de garanţie care poartă un asemenea simbol), chiar dacă este prezentat separat, în condiţiile referitoare la bunuri de la punctul (i);
(iii) materiale de ambalare care poartă marca bunurilor contrafăcute, prezentate separat, în aceleaşi condiţii ca bunurile de la punctul (i).

205 Vezi Raportul Organizaţiei pentru Cooperare şi Dezvoltare Economică (OCDE) intitulat *Impactul economic al contrafacerii şi pirateriei* (2007); documente ale INTERPOL Intellectual Property Crime Action Group (IIPCAG).

206 Vezi H. Reimers, *Regulation 1383/2003 and the effects of Border Detention on Intellectual Property Rights*, Master thesis, Faculty of Law, University of Lund, 2005.

BCU CLUJ CENTRAL UNIVERSITY LIBRARY

fenomen reprezintă circa 500 miliarde euro și între 7 și 10 % din comerțul internațional[207], site-urile web fiind adesea implicate în astfel de activități ilegale.

Contrafacerea comercială vizează produse din practic toate sectoarele economice, inclusiv cel al tehnologiei informațiilor și comunicatiilor[208]. Prin potențialul de a afecta foarte grav siguranța și/sau sănătatea consumatorilor[209], prin pierderi masive pe care le cauzează titularilor drepturilor de proprietate intelectuală și economiilor naționale, prin diminuarea locurilor de muncă[210], prin efectele negative asupra reputației, responsabilității[211] și competitivității firmelor, prin afectarea gravă a încrederii consumatorilor și, nu în ultimul rând, prin legăturile pe care le are cu crima organizată[212], contrafacerea comercială trebuie considerată va fiind un fenomen criminal deosebit de periculos și care trebuie combătut prin toate mijloacele. Pentru îmbunătățirea activității de combatere a infracțiunilor din domeniul proprietății intelectuale, a fost creată *Interpol Database on International Intellectual Property (DIIP) Crime*, o bază de date care conține informații despre crimele transnaționale și organizate.

3.1 Cadrul legal internațional

Există numeroase tratate internaționale în domeniul drepturilor de proprietate intelectuală, printre care:

• Convenția de la Berna[213]

---

207 Vezi European Parliament, *Draft Report on the impact of counterfeiting on international trade* [2008/2133(INI)], Rapporteur: G. Susta, 2008.

208 Un cetățean american care deținea Shoreline Networks a fost condamnat la 6 luni închisoare și o amendă de 150000 dolari pentru trafic cu produse pentru rețele informatice Cisco contrafăcute - Vezi detalii la locația http://www.cybercrime.gov (accesată 3 noiembrie 2008).

209 A se vedea, spre exemplu, șampon contrafăcut, care conținea acid, comercializat în Zambia; medicamente împotriva malariei contracufăcute, care au cauzat moartea mai multor persoane în Cambogia – vezi în H. Reimers, op. cit.; pastile falsificate, importate din China, au cauzat cel puțin 4 morți și 160 de îmbolnăviri în Japonia; medicamente contrafăcute, care au cauzat moartea a circa 192000 de persoane în China în 2001– vezi în The International AntiCounterfeiting Coalition, *Facts on fakes* (2005); siropul contra tusei care conținea antigel și care a cauzat peste 130 de decese în Panama, în 2006, menționat în G. Susta, *Raport referitor la impactul contrafacerii asupra comerțului internațional* (2008/2133(INI)) (2008).

210 Camera de Comerț a SUA estimează că produsele contrafăcute și cele piratate duc la pierderea de 750000 de locuri de muncă anual. Vezi și U.S. Homeland Security, *Intellectual Property Rights Seizures and Statistics, Fiscal Year 2013*, 2014.

211 Spre exemplu, un telefon mobil a explodat în timp ce folosea un încărcător contrafăcut – vezi în H. Reimers, op. cit.

212 Vezi The International AntiCounterfeiting Coalition, op. cit.; Commission of the European Communities, *Amended proposal for a Directive of the European Parliament and of the Council on criminal measures aimed at ensuring the enforcement of intellectual property rights*, 2006.

213 Vezi o discuție pe marginea acestei Convenții în M. Romițan, *Convenția de la Berna pentru protecția operelor literare și artistice – 120 de ani*, Revista Română de Dreptul Proprietății Intelectuale, III, 2 (7), 16-24, 2006.

- Convenţia de la Paris pentru protecţia proprietăţii industriale, în forma revizuită la Stockholm la 14 iulie 1967 (ratificată de România prin Decretul nr. 1777 din 28.12.1968)
- Tratatul de la Singapore privind dreptul mărcilor, 13-31 martie 2006 (ratificat de România prin Legea nr. 360 /4.12.2007)
- Tratatul privind cooperarea în domeniul brevetelor [*Patent Cooperation Treaty* (PCT)]
- Convenţia europeană privind brevetele [*European Patent Convention* (EPC)]
- Convenţia de la Stockholm privind instituirea Organizaţiei Mondiale a Proprietăţii Intelectuale (14 iulie 1967, ratificată de România prin Decretul nr. 1175 din 28.12.1968)
- Acordul privind constituirea Organizaţiei Mondiale a Comerţului
- Protocolul referitor la Aranjamentul de la Madrid privind înregistrarea internaţională a mărcilor adoptat la Madrid la 27 iunie 1989 (ratificat de România prin Legea nr. 5/1998)
- Aranjamentul de la Madrid privind înregistrarea internaţională a mărcilor, în forma revizuită la Stockholm la 14 iulie 1967 (ratificat de România prin Decretul nr. 1176 din 28.12.1968)
- Acordul general privind tarifele şi comerţul [*General Agreement on Tariffs and Trade* (GATT)][214]
- Tratatul privind mărcile de comerţ (*Trademark Law Treaty*)
- Aranjamentul de la Nisa privind clasificarea internaţională a produselor şi serviciilor în vederea înregistrării mărcilor din 15 iunie 1957, revizuit la Stockholm la 14 iulie 1967 şi la Geneva la 13 mai 1977 şi modificat la 2 octombrie 1979 (la care România a aderat prin Legea nr. 3/1998)
- Aranjamentul de la Viena instituind o clasificare internaţională a elementelor figurative ale mărcilor, întocmit la Viena la 12 iunie 1973 şi modificat la 1 octombrie 1985 (la care România a aderat prin Legea nr. 3/1998)
- Aranjamentul de la Strasbourg privind clasificarea internaţională a brevetelor de invenţie din 26 martie 1971, modificat la 28 septembrie 1979 (la care România a aderat prin Legea nr. 3/1998)
- Tratatul OMPI privind dreptul de autor [*WIPO Copyright Treaty* (WCT)]
- Convenţia universală asupra drepturilor de autor [*Universal Copyright Convention* (UCC)].

În mediul digital, numeroase companii îşi bazează activitatea pe modele de afaceri care presupun comercializarea de obiectele fizice ale proprietăţii intelectuale (purtătoare de drepturi de proprietate intelectuală). Spre exemplu, companii precum Amazon sau Barnes & Noble, care-şi desfăşoară activitatea online, utilizează baze de date uriaşe cu titluri de cărţi, înregistrări video, audio etc. În acelaşi timp, aceste companii deţin şi sisteme electronice de achiziţionare a

[214] Vezi negocierile Uruguay pentru actualizarea GATT.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

acestor produse, sisteme eficiente şi rapide prin care clienţii sunt atraşi de ele şi îndepărtaţi din tradiţionalele magazine.

Numeroase companii, mari sau mici, utilizează Internetul în această formă, adică în calitate de instrument de marketing pentru a informa potenţiali cumpărătorii despre propriile produse sau servicii. Clienţii pot accesa în orice moment ales, în mod individual şi din orice loc, magazinele virtuale ale acestor companii. În acest mod, are loc o "digitizare" a produselor purtătoare de drepturi de autor, un proces care reduce textul, grafica şi imaginile vizuale ori sunetele la un cod. Transformate în biţi, produsele pot "călători" de-a lungul reţelelor şi astfel proprietăţii intelectuale i se permite să fie transferată în mediul digital. Acest curent ascendent al migrării proprităţii intelectuale pe Internet l-a făcut pe faimosul comentator al Internetului şi fondator al Electronic Frontier Foundation, J. P. Barlow, să vorbească despre "digitizarea a tot ce se poate"215.

Pe măsură ce folosirea sistemelor informatice şi a Internetului îşi continuă evoluţia remarcabilă privind capacitatea de a disemina conţinut digital, sistemul de proprietate intelectuală a fost propulsat în centrul dezbaterii despre forma viitoare a lumii digitale. În acest mediu nou, în continuă schimbare, informaţia şi cunoasterea sunt resursele de bază, iar sistemul de proprietate intelectuală - corpul de reglementări ce ocroteşte creaţiile minţii - este considerat a avea un rol crucial în stabilirea unei fundaţii trainice pentru dezvoltarea societăţii informaţionale. În timp ce sistemul proprietăţii intelectale joacă un rol important în construirea noii lumi digitale, Internetul are şi va avea un profund efect asupra sistemului în sine.

Fiind un sistem complex, deschis, format din multe variabile, cu relaţii non-lineare care nu pot fi descrise, explicate sau prezise cu precizie, influenţele pe care le exercită pe termen lung sunt încă neclare. Noutatea marcantă a acestui nou mediu nu a permis realizarea unor studii empirice aprofundate, în consecinţă starea de incertitudine este normală ("viata este trăită înainte şi înţeleasă înapoi"). Cu toate acestea, ceea ce este evident şi imediat aparent, este faptul că noul mediu prezintă oportunităţi şi provocări complexe pentru comunitatea proprietăţii intelectuale.

Având în vedere aceste realităţi, Organizaţia Mondială a Proprităţii Intelectuale s-a angajat într-un vast şi complex program de activităţi, denumit Agenda digitală a Organizaţiei Mondiale a Proprităţii Intelectuale[216], care reflectă şi răspunde influenţelor Internetului şi tehnologiilor digitale asupra sistemului proprietăţii intelectuale şi vice-versa în anii care vin. Organizaţia Mondială a Proprietăţii Intelectuale s-a angajat să formuleze răspunsurile cele mai potrivite care urmăresc încurajarea diseminării şi exploatării lucrărilor rezultate din activitatea

[215] J. P. Barlow, *Selling Wine Without Bottles: The Economy of Mind on the Global Net, High Noon of the Electronic Frontier*, Conceptual Issues in Cyberspace (P. Ludlow, ed.), 9-10, 1996.

[216] A se vedea WIPO Digital Agenda, http://ecommerce.wipo.int, Electronic Commerce Program and activities. WIPO Digital Agenda a fost lansată în septembrie 1999 de directorul general al WIPO la Conferinţa Internaţională în domeniul Comerţului Electronic şi al Proprietăţii Intelectuale şi a fost aprobată la sfârşitul lunii septembrie 1999 de către statele membre la Adunarea Generală a Organizaţiei Mondiale a Proprietăţii Intelectuale.

BCU IASI CENTRAL UNIVERSITY LIBRARY

creativă şi a cunoaşterii în Internet, precum şi la protejarea drepturilor creatorilor lor - în acest mediu, aflat în evoluţie constantă, aceasta este cu adevărat o provocare.

Pentru continuarea dezvoltării comerţului electronic, este esenţială crearea şi menţinerea unui mediu stabil şi pozitiv. Un sistem puternic al proprietăţii intelectuale joacă un rol vital într-un asemenea mediu, aşa cum rezultă şi din rapoartele Organizaţiei Mondiale a Proprietăţii Intelectuale. Problema cheie în transformarea cu adevărat a noului mediu în unul propice dezvoltării afacerilor electronice şi protejării drepturilor titularilor este înţelegerea caracteristicilor şi naturii sistemului de proprietate intelectuală în cadrul acestui mediu digital.

Esenţial, caracterul sistemului de proprietate intelectuală este evoluţionar, şi în timp ce natura acestor drepturi, modul de control şi exploatare a produsele rezultate din procesul creativ şi inovativ rămân relativ constante, maniera în care acestea sunt exprimate şi schimbate trebuie constant adaptată la progresele înregistrate de tehnologiile prin care se realizează aceste operaţiuni. Astfel, invenţia tiparniţelor, a fonogramelor, a televiziunii şi a radioului, a transmisiei prin cablu şi satelit, a înregistrarilor video, pe CD, sau DVD şi a Internetului au afectat, în acelasi timp, forma şi substanţa drepturilor de proprietate intelectuală.

Prin natura lor adaptabile, produsele purtătoare de drepturi de proprietate intelectuală au migrat masiv spre Internet şi au fost modificate pentru a se potrivi cu mediul digital. Proprietatea intelectuală a căpătat importanţă în acest mediu pe măsură ce valorile din domeniul afacerilor sunt acum reflectate în forma virtuală. Valoarea multor companii virtuale, spre exemplu, poate fi găsită în uriaşele baze de date pe care le deţin, baze de date care cuprind informaţii despre clienţi. Aceste baze de date pot fi considerate subiect al protecţiei în domeniul proprietăţii intelectuale.

Comunitatea proprietăţii intelectuale incluzând creatori de muzică şi film, creatori de programe informatice, autori şi editori exploră acum căile prin care produsele lor să fie disponibile online, dar, în acelasi timp, să le fie protejate drepturile şi să-şi recupereze astfel investiţia făcută în activitatea creativă. Într-o anumită măsură, îndeplinirea acestui deziderat este dependentă de managementul strategic al acestor drepturi, de disponibilitatea unui sistem de securitate în domeniul procurării şi al plăţilor pentru produsele purtătoare de drepturi de proprietate intelectuală şi de crearea şi întretinerea încrederii consumatorilor în platile electronice, precum şi în apărarea confidenţialităţii datelor referitoare la clienţi.

Încercând să găsească o rezolvare pentru protejarea uniformă, la nivel înalt, a drepturilor creatorilor ale căror opere sunt disponibile pe Internet, cât şi pentru progresul afacerilor electronice, Uniunea Europeană a propus o Directivă în domeniul armonizării unor aspecte referitoare la drepturile de autor şi drepturile conexe în societatea informaţională încă din 25 mai 1999 (Directiva 2001/29/EC, numită şi *the Copyright Directive*). Directiva mentionată prezintă importanţă pentru toţi furnizorii (vânzătorii) implicaţi în tranzacţiile de comerţ electronic directe[217].

---

[217] Prin *tranzacţie de comerţ electronic directă* se înţelege acea tranzacţie în care Furnizorul (Vânzătorul) şi Cumpărătorul nu numai că încheie contractul prin Internet, dar îşi îndeplinesc toate obligaţiile reciproce ce derivă din contract tot via Internet ("online"). Acest tip de tranzacţie directă de comerţ electronic este posibilă numai dacă bunurile sau serviciile

În Directivă se arată cu claritate necesitatea protejării drepturilor de exclusivitate la distribuire a deţinătorilor drepturilor de autor. Pentru a crea însă o balanţă între necesitatea protecţiei drepturilor de autor, pe de o parte, şi facilitarea transferului şi reproducerii de date şi informatii protejate prin drept de autor la cursul normal al traficului Internet, pe de alta parte, s-au prevăzut excepţii în unele cazuri (reproduceri în scop necomercial de către persoane fizice, dar cu condiţia recompensării rezonabile a celui ce deţine dreptul de autor: reproducerea în scop de arhivare şi/sau conservare fără scop comercial, atunci când este realizată în cadrul bibliotecilor, arhivelor, ori în scop didactic, educaţional sau cultural; în cazul fixărilor efemere şi temporare, realizate de organizaţiile de transmitere a ştirilor, prin mijloacele pe care le deţin, pentru buletinele lor informative).

Directiva europeană în domeniul dreptului de autor cuprinde o listă de diferite limitări ale protecţiei în domeniu şi pe care statele membre pot să le stipuleze în legislaţiile lor naţionale în domeniu. Aceste limitări se referă la: învăţământ, promovarea operelor în domeniul artistic fără un interes comercial, comunicarea articolelor publicate în domeniul economic, politic sau religios. Directiva europeană enunţă şi obligaţia pentru fiecare din statele membre de a asigura protecţia legală pentru măsurile tehnice, în scopul prevenirii încălcării drepturilor de autor în mediul digital (spre exemplu, protecţia legală pentru criptarea programelor informatice şi filigrane tehnice) şi să prevadă pedepse pentru cei care produc mecanisme tehnice pentru a ocoli protecţia tehnică asigurată operelor purtătoare de drepturi de autor[218]. Eforturi regionale cum este cel al Uniunii Europene se integrează, de fapt, într-un efort global de rezolvare a oportunităţilor şi provocărilor legate de complexa legatură dintre afacerile electronice şi sistemul de proprietate intelectuală (Organizaţia Mondială a Proprietăţii Intelectuale a început încă din 2000 consultări regionale şi a organizat numeroase întâlniri cu privire la problemele ridicate de comerţul electronic şi de proprietatea intelectuală).

Cele mai importante aspecte sunt: identificarea problemelor de proprietate intelectuală ridicate de afacerile electronice şi formularea de politici potrivite pentru a răspunde acestor chestiuni; dezvoltarea şi adaptarea sistemelor de proprietate intelectuală, incluzând politicile regionale şi legislaţia, care nu numai că promovează progresul afacerilor electronice, dar protejează, în acelaşi timp, şi drepturile de proprietate intelectuală ale creatorilor autohtoni şi micile afaceri, încurajând şi dezvoltarea ţeconomică şi culturală, precum şi investiţiile; îmbunătăţirea sistemului de protecţie a proprietăţii intelectuale prin consiliere şi asistenţă tehnică; stabilirea unui sistem al numelor de domenii Internet prin politici

---

achiziţionate sunt intangibile şi toate etapele contractului sunt executate exclusis prin Internet sau prin alte mijloace electronice (cum ar fi SMS, fax sau alte forme de comunicare electronică). Spre exemplu, achiziţionarea de programe informatice, filme, muzică sau informaţie protejată, care sunt obţinute de cumpărător via Internet vor constitui *tranzacţii de comerţ electronic directe*.

[218] Toate aceste măsuri au fost prevăzute şi în legislaţia românească în domeniu; a se vedea Legea nr. 285/2004 care a modificat şi completat Legea nr. 8/1996 privind dreptul de autor şi drepturile conexe.

de înregistrare de catre autoritățile naționale; organizarea de campanii de educare și perfectionare în acest domeniu.[219]

3.2 Drept de autor și drepturi conexe

Prin drept de autor, pot fi protejate lucrări literare sau artistice, cum ar fi cărți, compoziții muzicale, programe pentru calculator etc. Principale rațiune a protecției prin drept de autor și drepturi conexe constă în încurajarea și răsplătirea lucrărilor creative.

3.2.1 Protecția programelor informatice

În epoca digitală, programele informatice joacă un rol esențial. Industria programelor informatice este un contributor foarte important la economia multor state, iar firmele din domeniu înregistrează creșteri anuale impresionante. În sectorul programelor informatice și al serviciilor asociate, sunt angajate milioane de persoane, iar contribuția la produsul intern brut depășește sute de miliarde dolari.

Conform Directivei 2009/24/CE, "program pentru calculator" ar trebui să includă programe indiferent de forma acestora, inclusiv cele care sunt încorporate în hardware. Această noțiune include, de asemenea, lucrările de concepție pregătitoare care au drept scop dezvoltarea unui program, cu condiția ca acestea să fie de natură să permită realizarea unui program pentru calculator într-un stadiu ulterior.

Crearea de programe pentru calculator necesită utilizarea unor resurse umane, tehnice și financiare foarte mari, în timp ce posibilitatea de a le copia există la un cost mult inferior. Vulnerabilitatea actuală mare a programelor informatice se datorează Internetului, globalizării și răspândirii în masă a calculatoarelor, din ce în ce mai puternice și mai ieftine, care fac ca programele informatice să poată fi piratate mult mai usor și pe zone geografice mult mai extinse[220].

Pirateria informatică reprezintă o preocupare majoră pentru industria programelor informatice datorită pierderilor financiare și, în unele cazuri, de imagine pe care aceasta le aduce. Pirateria informatică nu afectează doar producatorii—guvernele pierd taxe, iar consumatorii sunt expuși unor riscuri și plătesc prețuri mai mari pentru produsele legitime. Pierderile cauzate programelor comerciale de pirateria informatică sunt estimate la 58,8 miliarde de dolari anual[221]. Adițional, pirateria informatică ridică probleme semnificative privind securitatea sistemelor informatice[222].

---

[219] A se vedea pentru amănunte, WIPO Publication No.441E, Annual Report, 28, 2000.

[220] A se vedea *Convenția europeană privind criminalitatea informatică*, în special Raportul explicativ, Titlul 4 referitor la delictele împotriva drepturilor de proprietate intelectuală.

[221] A se vedea, Business Software Alliance, *Global Software Piracy Report*, 2011; vezi și A. Bronstad, *'Cracked' Software License Suit in China Could Prove Model*, National Law Journal, June 20, 2011. Vezi și Seung-Hwan Mun, *Reality Check: Rethinking the Global*

BOLYAI UNIVERSITY LIBRARY

3.2.1.1 Licențe informatice

Multiplicitatea formelor programelor informatice și abordarea legislativă non-liniară, au dus la o protecție mixtă a programelor informatice: protecție tehnică (*technical protection measures* sau *digital rights management*[223]) și prin mijloace legale (cel mai adesea prin prin drept de autor[224], dar și prin secrete comerciale sau bveret de invenție[225], în anumite condiții[226]). Un rol esențial în protecția drepturilor asociate cu programele informatice este jucat de *licențele de utilizare*[227]. Licențierea programelor informatice este unul dintre cele mai mari sectoare industriale în SUA: conform studiului *2008 Software 500*, veniturile totale estimate pentru cele mai mari 500 de companii din domeniul programelor informatice și al serviciilor asociate au ajuns la 451,8 miliarde dolari[228].

În SUA, conform *First Sale Doctrine* a *Copyright Act* 17 U.S.C. §101 și urm., un individ care achiziționează o copie autorizată poate folosi și vinde respectiva copie fără restricții din partea deținătorului dreptului de autor. Creatorii programelor informatice, pentru a evita aplicarea acestei Doctrine și a reține controlul asupra redistribuirii propriilor programe, au apelat la distribuirea în masă

Software Piracy Problem, International Telecommunications Policy Review, 20 (2), June, 1-26, 2013.

222 Vezi detalii în John F. Gantz și colab., *The Dangerous World of Counterfeit and Pirated Software*, 2013.

223 Vezi P. Samuelson și J. Schultz, *Should Copyright Owners Have To Give Notice Of Their Use Of Technical Protection Measures?*, Journal On Telecommunications & High Technology Law, Vol. 6, 41-75, 2007.

224 Vezi, spre exemplu, L. Determann, *Dangerous Liaisons – Software Combinations As Derivative Works? Distribution, Installation and Execution of Linked Programs under Copyright Law, Commercial Licenses and the GPL*, Berkeley Technology Law Journal, Iss. 21:4, 2006; S. L. Dogan și J. P. Liu, *Copyright Law and Subject Matter Specificity: The Case of Computer Software*, NYU Annual Survey Of American Law, Vol. 61, 2005.

225 A se vedea, în acest sens, S. Sterckx și J. Cockbain, *The Patentability of Computer Programs in Europe: An Improved Interpretation of Articles 52(2) and (3) of the European Patent Convention*, Journal of World Intellectual Property, Vol. 13, No. 3, 366–402, 2010; A. Iancu și P. Gratzinger, *Machines and Transformations: The Past, Present, and Future Patentability of Software*, Northwestern Journal Of Technology And Intellectual Property, Vol. 8, 2010; R. A. McFarlane și T. V. Fisher, *Software Patents Under 35 U.S.C. § 271(F): Should Congress Amend § 271 To Harmonize Protection Between Tangible And Intangible Inventions?*, 2 Hastings Science And Technology Law Journal, 183, 2010; European Patent Office, *Patents for Software?*, 2009; L. Pallas Loren, *The Pope's Copyright? Aligning Incentives with Reality by Using Creative Motivation to Shape Copyright Protection*, Louisiana Law Review, Vol. 69, 2008; R. P. Merges, *Software and Patent Scope: A Report from the Middle Innings*, Texas Law Review, Vol. 85, 2007; P. Leith, *Software and Patents in Europe*, Cambridge University Press, 2007.

226 A se vedea Decizia Curții Supreme din SUA în *Alice Corp. v. CLS Bank* (2014).

227 Vezi, spre exemplu, H. Travis, *The Principles of the Law of Software Contracts: At Odds with Copyright, Consumers, and European Law?*, Research Paper No. 10 – 01 (2010); D. Tollen, *The Tech Contracts Handbook: Software Licenses and Technology Services Agreements for Lawyers and Business People*, 2010; J. I. Gordon, *Software Licensing Handbook*, 2008.

228 Conform M. L. Rustad și M. V. Onufrio, *The Exportability of the Principles of Software: Lost in Translation?*, Hastings Science & Technology Law Journal, 2010.

BUCHAREST UNIVERSITY LIBRARY

a programelor cu *licenţă de folosire*, nu prin vânzare directă[229]. Distincţia între vânzarea şi licenţierea unui program informatic nu este întotdeauna clară (cu implicaţie directă dacă un utilizator al unui program licenţiat este deţinătorul unei copii particulare), lucru reflectat şi într-un caz din SUA: *Vernor v. Autodesk, Inc.*[230].

O **licenţă** pentru un program informatic, numită, cel mai adesea, *Software License Agreement* (SLA) sau *End-User License Agreement* (EULA)[231], este un instrument legal, considerat a se afla la intersecţia doctrinelor privind contractele, proprietatea intelectuală şi dreptul comercial[232], care stipulează drepturile şi obligaţiile utilizatorului (parametrii de utilizare) în conexiune cu programul informatic în cauză (care poate fi o aplicaţie, un sistem de operare sau un server). Licenţele de utilizare a programelor informatice pot fi negociate între părţi[233] sau standard[234], de tip *shrink-wrap* (vizibilă prin celofanul care acoperă pachetul care conţine suportul pe care este stocat programul informatic şi care prevede că deschiderea pachetului presupune acceptarea termenilor licenţei) sau *click-wrap* (similară cu cea anterioară, dar vizibilă online, programul informatic în cauză putând fi descărcat de pe o locaţie Internet)[235].

---

229 Vezi cazuri decise în instanţă, în care doctrina primei vânzări nu se aplică programelor informatice licenţiate: Microsoft Corp. v. Software Wholesale Club, Inc,, 129 F.Supp.2d 995 (S.D. Tex. 2000); Adobe Systems, Vnc. v. One Stop Micro, Inc., 84 F. Supp. 2d 1086, 1089 (N.D.Cal. 2000). Vezi şi J. W. Newman, *Selling the Right to License: Examination of the First Sale Doctrine Through the Lens of UMG Recordings & Quanta Computer*, Journal of Corporation Law, Vol. 35, 2010; M. Flumenbaum şi B. S. Karp, *Copyright Law: When Customer 'Owns' Copy of Computer Program*, New York Law Journal, Vol. 233, No. 80, 2005.

230 Vezi detalii în M. Halpern, Y. Kapgan şi K. Yu, *Vernor v. Autodesk: Software and the First Sale Doctrine under Copyright Law*, Intellectual Property & Technology Law Journal, Vol. 23, No. 3, March, 2011; R. Raysman şi P. Brown, *First Sale of Licensed Software*, New York Law Journal, November 10, 2010; *Impenatrable EULAs and the Dying First Sale Doctrine: Vernor v. Autodesk*, September 10 (2010), comentariu disponibil la http://www.technicallylegal .org/impenatrable-eulas-and-the-dying-first-sale-doctrine-vernor-v-autodesk/; C. M. Mills, *When is a Software License Actually a Sale? A New District Court Decision Addresses the Copyright First Sale Doctrine and Software*, Intellectual Property Insights, Fall, 2008. În acest context, a se vedea şi cazul Softman Products Company, LLC v. Adobe Systems, Inc., în care a fost implicat un *reseller*, nu un utilizator (*end-user*).

231 A se vedea A. Guadamuz, *The Rise and Rise of the Software Licence*, Journal of Intellectual Property Law & Practice, Vol. 6, No. 2, February, 128-129, 2011; M. L. Rustad, *Software Licensing: Principles and Practical Strategies*, Research Paper 10-49, 2010; D. E. Phillips, *The Software License Unveiled: How Legislation by License Controls Software Access*, 2009; E. I. Winston, *Why Sell What You Can License? Contracting Around Statutory Protection of Intellectual Property*, 14 George Mason Law Review, 2006; M. J. Madison, *Reconstructing the Software License*, Loyola University Chicago Law Journal, Vol. 35, 2003.

232 Vezi Michael L. Rustad, *Software Licensing*, op. cit.

233 Vezi N. M. Kim, *The Software Licensing Dilemma*, Brigham Young University Law Review, 2008.

234 Vezi R. W. Gomulkiewicz, *Getting Serious About User-Friendly Mass Market Licensing For Software*, George Mason Law Review, Vol. 12, 2004.

235 Vezi discuţii despre aceste tipuri de licenţe în N. S. Kim, *Clicking and Cringing*, Oregon Law Review, Vol. 86, 2007; K. W. Swanson, *"Click to Accept": When is an enforceable contract formed?*, Intellectual Property & Technology Law Journal, Jun, 2002.

După cum observă Rao şi colab.[236], licenţele de folosire a programelor informatice sunt utilizate pentru a asigura respectarea drepturilor de proprietate intelectuală ale deţinătorului prin obligarea utilizatorului să admită validitatea respectivelor drepturi şi furnizarea unui instrument legal adiţional privind domeniul sau termenii de folosire a programului informatic în cauză. În general, licenţele prevăd numărul de copii permise ale programului şi drepturile de a mări sau scădea drepturile acordate (*upgrade* sau *downgrade*). Licenţele limitează adesea folosirea programului informatic în cauză doar pentru scopuri interne (*internal business purpose only*, expresie ambiguă, folosită pentru a limita folosirea programului).

Majoritatea licenţelor pentru programe informatice sunt "nonexclusive", pentru a putea licenţia acelaşi program informatic şi altor persoane, dar se întâlnesc şi situaţii în care termenii licenţei prevăd folosirea exclusivă a programului informatic (spre exemplu, în situaţiile în care folosirea acestuia consituie un avantaj competiţional sau dacă programul informatic este folosit în anumite sectoare industriale sau zone geografice)[237]. O altă limitare des întâlnită în licenţele de folosire a programelor informatice se referă la folosirea pe un anumit calculator sau unitate centrală (CPU), pe un anumit grup de calculatoare sau la o anumită locaţie geografică. Licenţele pot fi *perpetue* sau *irevocabile* (acestea sunt valide pentru totdeauna dacă programul informatic este folosit în acord cu termenii licenţei), *temporare* sau *non-perpetue* (numite şi *subscription licenses*, care sunt valide pe o perioadă predefinită), de tip "întreţinere" (*maintenance*, care permite utilizatorului să primească noi versiuni ale programului pe durata convenită cu devzoltatorul programului) sau de tip *pay-per-use*.

Licenţele conţin, adesea, specificaţii privind funcţionalităţile disponibile ale programului: ce funcţionalităţi pot fi (sau nu pot fi) folosite, durata pentru care anumite funcţionalităţi pot fi folosite şi/sau numărul de sesiuni care pot fi executate într-o anumită perioadă şi specificaţii funcţional şi tehnice (care pot descrie elemente fizice şi de programare, inclusiv performanţa şi fiabilitatea estimată a programului informatic).

Licenţele pot fi acordate pentru un singur utilizator (*Single User*) sau partajate (*Multi-User Shared*, care permit partajarea folosirii programului informatic între mai multe persoane, de regulă angajaţi ai unui organizaţii) sau pot fi asociate cu un anumit calculator (*node-locked*), cheie fizică (*dongle*), site (locaţie) sau utilizator (drepturile de folosire sunt asociate cu un anumit *ID* la log-are; altfel spus, *per-user*, *per-procesor* sau *per-socket*[238]), flotante (*floating*, în care drepturile de folosire sunt legate de o anumită listă de calculatoare) sau concurente (*Concurrent Device*, care definesc numărul maxim de periferice care pot fi conectate la un sistem desemnat concurent).

---

236 Vezi P. M. Rao, E. A. Borg şi J. Klein, *The Information and Communication Technologies and Enforcement of Intellectual Property Rights: A Relationship Perspective*, Journal of World Intellectual Property, Vol. 11, No. 2, 105–119, 2008.

237 Vezi consideraţii pe această temă în H. Ward Classen, *A Practical Guide to Software Licensing for Licensees and Licensors*, 2nd Ed., 2007.

238 Vezi, spre exemplu, schema de licenţiere a produselor Oracle la locaţia http://www.orafaq.com/wiki/Oracle_Licensing.

BCU IASI CENTRAL UNIVERSITY LIBRARY

Licențele de utilizare pot acorda drepturi *limitate* sau *nelimitate* (pentru o perioadă de timp, numite *Unlimited License Agreements*). Licențele pot privi un program informatic, pot face referire la pachete de programe (*packages* sau *bundling*) sau pot fi eterogene (*heterogeneously licensed* sau HtL), cu diferite componente guvernate de licențe diferite[239]. Licențele de utilizare pot adresa o "ediție" (care oferă funcționalități diferite în cadrul unui produs informatic) sau o "versiune" (o anumită generație a unui produs informatic) a unui program informatic.

Licențele de utilizare au termeni diferiți, în funcție de destinația programului informatic. Astfel, putem vorbi despre programe distribuite în volume mari (*Volume Licensing Programs*), programe destinate productorilor de echipament informatic (*Original Equipment Manufacturer*), programe destinate mediului educațional, produse de tip *Full Packaged Product* (FPP), producători independenți de programe informatice (*Independant Software Vendors*, care includ tehnologii licențiate în propriile produse) sau situații în cadrul cărora părțile acceptă schimbul de drepturi (*cross licensing*).

Licențele de folosire rareori permit reproducerea sau modificarea programelor informatice în cauză, adaptarile programului informatic nu pot fi transferate fără permisiunea deținătorului dreptului de autor, iar deținătorul unei copii a unui program informatic nu poate închiria sau împrumuta copia unei terțe parți fără permisiunea deținătorului dreptului de autor asupra programului informatic în cauză[240]. Adițional, licențele pot să limiteze responsabilitățile[241] producătorului privind potrivirea programului info rmatic la anumite scopuri, performanțele acestuia sau obligația de a furniza suport, întreținere sau instalare, corectarea erorilor, actualizări sau alte modificări[242], pot institui restricții privind divulgarea unor informații legate de programul informatic în cauză[243], realizarea de lucrări derivate[244] sau decompilarea[245].

Termenii licențelor sunt adesea considerați dificil de înțeles, iar anumite prevederi ale licențelor de utilizare a programelor informatice, cum ar fi interzicerea criticării publice a produsului, impunerea acceptării de fi monitorizat în urma folosirii produsului, interzicerea decompilării, interzicerea folosirii

---

[239] Vezi o discuție pe această temă în Thomas A. Alspaugh, Hazeline U. Asuncion și Walt Scacchi, *Presenting Software License Conflicts through Argumentation*, 2011.

[240] A se vedea, în acest context, și *Computer Software Rental Amendments Act* din 1990.

[241] Vezi, spre exemplu, un comentariu în S. S. Gilstrap, *Burden Shifting in Software Licensing Agreements*, 121 Yale Law Journal, 2011; vezi și T. R. Beard, G. S. Ford, T. M. Koutsky, L. J. Spiwak, *Tort liability for software developers: A law & economics perspective*, Journal Of Computer & Information Law, Vol. XXVII, 2009.

[242] Vezi, spre exemplu, *End User License Agreement for iContact for "Android"*, care stipulează lipsa obligației de a furniza întreținere sau instalare de orice tip, corectarea erorilor, updatări sau alte modificări.

[243] Vezi R. A. Hillman și M. O'Rourke, *Defending Disclosure in Software Licensing*, University of Chicago Law Review, 2011.

[244] Vezi, spre exemplu, N. Heineman, *Computer Software Derivative Works: The Calm Before the Storm*, Journal Of High Technology Law, Vol. VIII, No. 2, 2008.

[245] Vezi o discuție pe această temă în P. Samuelson și S. Scotchmer, *The Law and Economics of Reverse Engineering*, Yale Law Journal, Vol. 111, 2002.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

produsului cu alte produse, impunerea acceptării de modificări în versiuni ulterioare sau declinarea oricărei responsabilități în cazul în care produsul cauzează probleme pe calculatorul pe care este instalat, sunt considerate excesive sau chiar dăunătoare în literatura de specialitate [246]. Nerespectarea termenilor licențelor de utilizare duce, adesea, la dispute rezolvate în instanțe[247], uneori sumele acordate drept despăgubire fiind impresionante[248]. Adesea, chiar în situațiile în care termenii licenței sunt negociați direct, părțile implicate îi pot interpreta diferit[249]. Cazuri speciale apar în situațiile în care partea licențiată pentru folosirea unui program informatic intră în insolvență/faliment[250], debitorul având alternativa între a rejecta sau păstra licența (cu implicațiile asociate), sau în situațiile de preluare a firmelor care dețin licența de utilizare[251].

3.2.1.2 Protecția tehnică

Principalele tehnici de protecție tehnică a programelor informatice includ:

Inserarea de semne sau informații secrete (*software watermarking*): Tehnică de protecție a programelor informatice prin inserarea de semne sau

---

246 Vezi, spre exemplu, J. T. Kunze, *Regulating Virtual Realms Optimally: The Model End User License Agreement*, Northwestern Journal of Technology and Intellectual Property, Iss. 1, Fall, 2008; A. Newitz, *Dangerous Terms: A User's Guide to EULAs*, 2005.

247 Vezi Apple Inc. v. Psystar Corp. (N.D.Cal. 12-15-2009): Sistemul de operare Mac OS X, fie preinstalat, fie stocat pe un DVD, este licențiat, nu vândut utilizatorului de către Apple Inc., pentru folosire conform termenilor Licenței; Oracle USA, Inc. v. Rimini Street, Inc. (Nev. 10-29-2010): În acest caz, Oracle a acuzat firma Rimini Street că a descărcat ilegal programe informatice și materiale asociate prin log-are la baze de date protejate prin parolă ale Oracle folosind parola unui client și descărcarea de materiale care depășesc autorizarea acordată de licență acelui client; Microsoft Corp. v. Aga Solutions (E.D.N.Y. 3-22-2010); vezi și R. T. Nimmer, *An Essay on Article 2's Irrelevance to Licensing Agreements*, Loyola Of Los Angeles Law Review, Vol. 40, 2006.

248 Vezi, spre exemplu, cazul Oracle Corp. v. SAP AG (N.D. Cal. 8-17-2010), în care s-a acordat o compensație de 1,3 miliarde dolari.

249 Vezi, spre exemplu, *Sun Microsystems, Inc. v. Microsoft Corp.*: inițial părțile au intrat într-un acord care prevedea licențierea, fabricarea și distribuirea de produse bazate pe tehnologii Java; ulterior, Microsoft a realizat modificări neautorizate ale librăriilor de clase Java și nu a inclus suport pentru o tehnologie care trebuia să permită programelor scrise în limbajul de programare Java să lucreze cu alte sisteme de operare decât cele realizate de Microsoft.

250 Vezi N. S. Hirshman, M. G. Fatall și P. M. Spingola, *Is Silence Really Golden? Assumption and Assignment of Intellectual Property Licenses in Bankruptcy*, Hastings Business Law Journal, Vol. 3, 2007; W. E. Agin, *Drafting the Intellectual Property License: Bankruptcy Considerations*, Journal Of Bankruptcy Law And Practice, Vol. 9, 2000.

251 Vezi, spre exemplu, cazul *Cincom Systems v. Novelis Corp.*, în care s-a susținut că licența de utilizare a fost transferată în mod neautorizat, discutat în M. A. Esquenet, *Use of Software License after Merger Was an Unauthorized License Transfer and Copyright Infringement*, Journal of Intellectual Property Law & Practice, March, 2010; H. J. Pace, *Anti-Assignment Provisions, Copyright Licenses, and Intra-Group Mergers: The Effect of Cincom v. Novelis*, Northwestern Journal of Technology and Intellectual Property, Vol. 9, No. 3, 2010.

informații pentru a identifica deținătorul drepturilor de autor[252]. Funcțiile protective pot fi un semn sau informație de *validare*, de *licențiere* sau de *identificare*.

Cod de activare: reprezentat de o serie de litere și numere, care trebuie introduse la lansarea programului informatic. Codul este furnizat la cumpărarea produsului, este obținut prin apelarea telefonică a deținătorului produsului sau prin intermediul Internet (prin introducerea unui număr serial, care permite producătorului să obțină informații despre locația și tipul programului informatic instalat, în vederea prevenirii instalării programului informatic folosind același număr serial). Programul informatic nu va porni sau va lansa o versiune simplificată, dacă nu este introdus codul de activare corect.

Cheie fizică: Folosirea unei "chei fizice" (numită, în literatura de specialitate sau printre practicieni, *dongle*, *hardware key*, *hardware token* sau *security device*), adică a unui dispozitiv fizic care conține un număr serial și poate fi conectat la un calculator pentru a autentifica un program informatic (pentru a preveni copierea sau rularea abuzivă). În cazul absenței dispozitivului de protecție, programul informatic va rula în mod restrictiv sau nu va rula deloc. Dispozitivele moderne includ criptare puternică incorporată și mecanisme care împiedică decompilarea. De asemenea, aceste dispozitive pot conține memorii non-volatile, astfel încât anumite părți ale programelor informatice pot fi stocate și executate pe dongle. *iLok* (*Copy Protection*), *Syncrosoft* și *Matrix Software License Protection System* sunt dispozitive de protecție care folosesc un port USB pentru conectare.

Management de licențe: Există mai multe posibilități de licențiere a programelor informatice. Astfel, un program informatic poate fi asociat cu un anumit calculator (*node-locked*), permițându-i-se să ruleze numai pe respectivul calculator; un program informatic poate fi asociat cu un număr de licențe flotante, alocate dinamic calculatoarelor. *FLEXlm* este un exemplu de program care acționează ca un manager de licențe și care suportă ambele modele. FLEXlm este folosit în medii de afaceri cu multe sisteme informatice, pentru a furniza licențe flotante către un număr de utilizatori predefinit ai unui program informatic.

Protecție împotriva copierii: Mecanismele de protecția împotriva copierii leagă programul informatic instalat de un anumit calculator prin implicarea unor caracteristici unice ale acestuia: număr serial ROM, data și momentul inițializării discului dur, adresa MAC (pentru calculatoare cu card Ethernet) sau a altor numere specifice unui calculator. Unele programe informatice au mecanisme de protecție mai sofisticate. Astfel, Microsoft Xbox are o funcție specifică împotriva copierii: *non-booting* sau *non-citire* de pe CD și DVD-R. Playstation 2 are un fișier care conține informații privind poziția exactă I dimensiunea fișierelor pe CD, jocul apelând poziția la care trebuie să se afle fișierul. Nintendo Wii și Gamecube au propriul format împotriva copierii, bazat pe o tehnologie DVD/miniDVD (Game Cube): pe marginea discului există un cod de bare, care nu poate fi citit pe periferice DVD-ROM standard.

Obscurizarea codului sursă: Secretele incorporate într-un program informatic pot include algoritmi, subrutine, constante ș.a. Codul obscurizat

---

[252] Vezi W. Zhu și C. Thomborson, *Recognition in software watermarking*, Proceedings of the 4th ACM international workshop on Contents protection and security, 29 – 36, 2006.

(*obfuscation*) este realizat pentru a contracara riscurile legate de accesul neautorizat la codul sursă. Codul obscurizat este cod sursă astfel realizat încât este greu sau chiar imposibil de citit/înțeles. Există o mare varietate de tehnici de obscurizare, mergând de la simpla substituire a unor cuvinte-cheie, folosirea de spații, programe auto-generante sau compresate masiv, obscurizarea fluxului de control al programului, obscurizarea identificatorilor, cod auto-modificant, obscurizarea de date etc.[253].

Există, de asemenea, programe care operează asupra codului sursă, codului obiect sau a ambelor, pentru a nu permite decompilarea. Obscurizarea prin modificarea codului (*code morphing*) se referă la obscurizarea codului obiect, realizată prin înlocuirea completă a secțiunii de cod compilat cu un nou bloc care presupune aceeași stare la începerea execuției ca în secțiunea precedentă și care lasă aceeași stare de execuție după terminare, ceea ce face mult mai dificilă decompilarea programului informatic distribuit. Acest mecanism este folosit și pentru a determina autenticitatea copiei folosite.

3.2.1.3 Protecția legală

Literatura de specialitate a analizat diferitele instituții legale sub care pot fi protejate programele informatice: drept de autor, secrete comerciale, drept contractual, dreptul brevetelor, dreptul mărcilor etc. Pentru a fi protejat prin brevet, un program informatic trebuie să fie considerat o invenție. Majoritatea programelor informatice nu îndeplinesc această cerință și sunt protejate prin drept de autor, care conferă o protecție imediată[254]. Scopul principal al dreptului de autor nu este, cum cred mulți, să protejeze autorii împotriva insușirii roadelor muncii și creativității lor, ci să promoveze progresul științei și al artelor, prin asigurarea autorilor și inventatorilor de drepturi exclusive pentru lucrările lor. Această protecție este esențială pentru oferirea de motivații materiale pentru crearea de lucrări noi.

Cele mai importante tratate internaționale referitoare la protecția prin drept de autor sunt Convenția de la Berna (cu toate că în această Convenție nu sunt explicit incluse programele informatice, definiția operelor literare și artistice este foarte largă și poate include și programele informatice); Convenția Universală a Drepturilor de Autor (*the Universal Copyright Convention*); Tratatul OMPI asupra Drepturilor de autor (din anul 1996, care stipulează explicit că programele informatice sunt protejate ca opere literare, conform Convenției de la Berna); anumite prevederi ale Acordului TRIPS (*Trade-Related Aspects of Intellectual*

---

[253] Vezi H. Yamauchi și colab., *Software obfuscation from crackers' viewpoint*, Proceedings of the IASTED International Conference Advances in Computer Science and Technology, January 23-25, 2006; B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan and K. Yang, *On the (im)possibility of obfuscating programs*, Advances in Cryptology, 1-18, 2001.

[254] Vezi, spre exemplu, A. Guadamuz González, *The software patent debate*, Journal of Intellectual Property Law & Practice, 1(3), 196-206, 2006; H. C. Wegner, *Recent software patent protection trends*, SOFTIC, Tokyo, Japonia, 2005.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

Property Rights)[255] [spre exemplu, secțiunea "Copyright and Related Rights", articolele 10(1), 10(2), 11 și 13] și Directiva Consiliului European din 14 mai 1991 (*Directive on the Legal Protection of Computer Programs*, amendată în 2009, vezi mai jos).

Conform Directivei 2009/24/CE a Parlamentului European și a Consiliului din 23 aprilie 2009 privind protecția juridică a programelor informatice, protecția se aplică oricărei forme de exprimare a unui program informatic, ideile și principiile care se află la baza unui element al oricărui program informatic, inclusiv cele care se află la baza interfețelor sale, nu sunt protejate de dreptul de autor ("program informatic" include materialul de concepție pregătitor). Conform art. 1 (3), un "program informatic" este protejat dacă este original, în sensul că reprezintă o creație intelectuală proprie autorului. Niciun alt criteriu nu se aplică pentru a stabili dacă acesta poate beneficia de protecție.

Drepturile exclusive ale titularului cuprind dreptul de a efectua sau de a autoriza (art. 4): reproducerea permanentă sau provizorie a unui program pentru calculator, în totalitate sau parțial, prin orice mijloc și sub orice formă. În măsura în care încărcarea, prezentarea, rularea, transmiterea sau stocarea programului pentru calculator necesită o astfel de reproducere a programului, aceste acte de reproducere sunt supuse autorizării de către titularul dreptului; traducerea, adaptarea, dispunerea și orice altă transformare a programului pentru calculator și reproducerea rezultatelor acestor acte, fără a aduce atingere drepturilor persoanei care transformă programul pentru calculator; orice formă de distribuție publică, inclusiv închirierea originalului sau a copiilor unui program pentru calculator. Excepțiile la aceste drepturi privesc utilizarea programului (inclusiv corectarea erorilor) realizarea unei copii de rezervă (art. 5) și decompilarea (art. 6).

Conform art. 7, măsuri adecvate împotriva persoanelor care săvârșesc unul dintre următoarele acte: punerea în circulație a copiei unui program pentru calculator cunoscând sau având motive întemeiate să cunoască că este contrafăcută; deținerea în scopuri comerciale a copiei unui program pentru calculator cunoscând sau având motive întemeiate să cunoască că este contrafăcută; punerea în circulație sau deținerea în scopuri comerciale a oricărui mijloc având drept unic scop facilitarea eliminării neautorizate sau neutralizarea oricărui dispozitiv tehnic care poate fi instalat pentru protejarea unui program pentru calculator. Orice copie ilegală contrafăcută a unui program pentru calculator poate fi confiscată în conformitate cu legislația statului membru respectiv. Dispozițiile acestei directive nu aduc atingere altor dispoziții legale, cum ar fi, mai ales, cele privind brevetele, mărcile, concurența neloială, secretul comercial, protecția semiconductoarelor sau dreptul care guvernează contractele.

În România, protecția programelor informatice este guvernată de Legea nr. 8 din 1996, privind dreptul de autor și drepturile conexe[256]. Prin "program pentru calculator" (program informatic) se înțelege orice "expresie a unui program,

---

[255] Vezi, spre exemplu, S. A. Mota, *TRIPS: Ten Years of Disputes at the WTO*, Computer Law Review and Technology Journal, Vol. IX, NO. 3, 455-478, 2005.

[256] Modificată prin mai multe acte normative, vezi http://www.cdep.ro/pls/legis/legis_pck.htp_act?ida=8547.

programele de aplicaţie şi sistemele de operare, exprimate în orice fel de limbaj, fie în cod-sursă sau cod-obiect, materialul de concepţie pregătitor, precum şi manualele", "ideile, procedeele, metodele de funcţionare, conceptele matematice şi principiile care stau la baza oricărui element dintr-un program pentru calculator, inclusiv acelea care stau la baza interfeţelor sale, nu sunt protejate".

Autorul unui program informatic beneficiază îndeosebi de dreptul *exclusiv* de a realiza şi autoriza reproducerea permanentă sau temporară a unui program informatic, integral sau parţial, prin orice mijloc sau formă, traducerea, adaptarea, aranjarea sau orice alte transformări ale programului informatic, difuzarea originalului sau a copiilor programului informatic sub orice formă, inclusiv prin închiriere (punerea la dispoziţie spre utilizare, pentru un anumit timp şi pentru un avantaj economic sau comercial, direct sau indirect). Instalarea, stocarea, rularea sau executarea, afişarea ori transmiterea într-o reţea informatică a unui program informatic fără autorizarea titularului dreptului de autor reprezintă infracţiune şi se pedepseşte cu închisoare sau cu amendă.

Legea română permite realizarea unei copii de arhivă şi reproducerea codului sau traducerea formei sale atunci când aceste operaţiuni sunt indispensabile pentru obţinerea informaţiilor necesare interoperabilităţii unui program informatic cu alte programe informatice, dacă sunt îndeplinite condiţii cum ar fi deţinerea dreptului de utilizarea a unui copii a programului informatic, limitarea la părţile de program necesare interoperabilităţii, nedifuzarea informaţiilor astfel obţinute sau producerea sau comercializarea unui program informatic a cărui expresie este fundamental similară. Drepturile patrimoniale asupra programelor pentru calculator durează tot timpul vieţii autorului, iar după moartea acestuia se transmit prin moştenire, potrivit legislaţiei civile, pe o perioadă de 70 de ani. Reglementările din domeniu sunt completate de Ordonanţa Guvernului nr. 124 din 2000, aprobată cu modificări prin Legea nr. 213 din 2002. Această Ordonanţa consideră contravenţii faptele de distribuire, comercializare sau închiriere neautorizată de programe informatice, adică desfăşurarea de astfel de activităţi cu încălcarea obligaţiei de înregistrare în Registrul Programelor de Calculator (administrat de către Oficiul Român pentru Drepturile de Autor).

Potrivit Art. 139[9] din Legea nr. 8/1996 (modificată şi completată de Legea nr. 187/2012 pentru punerea în aplicare a Legii nr. 286/2009), se consideră infracţiune "101reproducerea neautorizată pe sisteme de calcul a programelor pentru calculator în oricare dintre următoarele modalităţi: instalare, stocare, rulare sau executare, afişare ori transmitere în reţea internă". Aceşti termeni au următorul înţeles:

- *Instalare*: configurarea unui nou program de calculator, în conformitate cu cerinţele sistemului, sau configurarea sistemului conform preferinţelor unui utilizator;
- *Stocare*: operaţiunea de păstrare a datelor şi a programelor informatice; pentru stocare există suporturi fizice (spre exemplu, discuri dure, flexibile sau compact, benzi magnetice etc.), care păstrează date sau programe informatice;

BCU IASI CENTRAL UNIVERSITY LIBRARY

- *Rulare sau executare*: operaţia de executare a secvenţei de instrucţiuni a unui program informatic;
- *Afişare*: prezentarea informaţiei într-o formă lizibilă, direct interpretabilă de către utilizator şi modificabilă la acţiunea acestuia sau a sistemului informatic; sau
- *Transmitere în reţea*: trimiterea datelor dintr-o anumită locaţie informatică în alta, cu ajutorul unui circuit de transmisie a datelor[257].

Pirateria informatică

Exită mai multe forme de bază ale pirateriei informatice, cu o incidenţă diferită, dar dăunătoare în toate formele:

Pirateria utilizatorului final, care poate lua următoarele forme:

- Folosirea unei copii legale pentru a instala un program pe mai multe calculatoare (dăpăşind număr de copii permis de licenţa existentă);
- Copierea discurilor în scopul instalării multiple sau în vederea distribuţiei;
- Exploatarea de oferte de actualizare fără a deţine o copie legală a versiunii care urmează să fie actualizată;
- Obţinerea frauduloasă a unor programe informatice cu destinaţie academică sau restricţionată (spre exemplu, NFR (*Not for Resale*), sau programe în regim Original Equipment Manufacturer (*OEM software*));
- Închirierea programelor informatice;
- Vânzarea sau licitarea unui program informatic în condiţii contrare prevederilor licenţei.

Pirateria online: Aceasta are loc atunci când un program informatic este încărcat pe Internet (situri web sau mall-uri warez) sau de pe reţele informatice (spre exemplu, *peer-to-peer*), astfel încât acesta poate fi obţinut de persoane neautorizate.

Pirateria producătorului de calculatoare: Instalarea de copii ale programelor informatice fără permisiune sau încălcând termenii acordului OEM.

Contrafacerea: Acest tip de piraterie este reprezentat de copierea ilegală şi vânzarea de materiale protejate prin drept de autor, cu intenţia de a imita direct produsul original, cel mai adesea CD-uri contrafăcute, incluse în pachetele cu materiale aferente: manuale, acorduri de licenţă, etichete, carduri de înregistrare şi caracteristici de securitate.

3.2.2 Protecţia operelor de artă digitală

Transmiterea extrem de facilă o operei de la creator la consumatorul de artă, sau între consumatorii de artă, a făcut din Internet un mediu ideal pentru diseminarea creaţiilor artistice. Un număr de caracteristici încurajează folosirea extensivă a mijloacelor digitale[258] (*inter alia*): natura intangibilă, foarte potrivită

[257] Vezi definiţiile din L. C. Christie şi J. Christie, *The Enciclopedia of Microcomputer terminology*, Prentice Hall, 1984.

[258] Vezi OECD, *Digital delivery of business services*, 2004.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

pentru transmitere digitală, eficiența sporită și costuri de transmitere foarte reduse, posibilitatea de expansiune economică etc. Tehnologiile existente furnizează mijloace noi și variate, destinate inovațiilor în toate domeniile, inclusiv în artă, dar, în acelasi timp, ridică multe provocări pentru proprietatea intelectuală[259].

O dată cu dezvoltarea tehnologiilor informației, arta a căpătat un nou înțeles și noi dimensiuni. Datorită întrepătrunderii cu tehnologiilor informației, a primit noi denumiri, greu de explicat și usor de confundat de cei ce nu sunt practicienii în acest domeniu. Astfel, "arta digitală", "arta digitizată", "arta electronică", "arta pe calculator", "arta ajutată de calculator", "arta pe Internet", "opera de artă digitală", "software pentru artă", etc. sunt termeni nou născuți din această întrepătrundere și care nu și-au găsit încă locul în dicționare riguros întocmite. Și-au făcut loc, însă, în texte de lege, fără să fie, din păcate, însoțiți de explicațiile absolut necesare, așa cum s-ar fi cuvenit, având în vedere noutatea lor. Astfel, expresia "operă de artă digitală" fost introdusă în Legea română a dreptului de autor și a drepturilor conexe, nr. 8/1996, prin completarea art. 7 (în anul 2004).

Pentru interpretarea corectă a textului de lege și aplicarea lui judicioasă în cazurile specifice din practică, vom încerca, în cele ce urmează, o "decodare" a termenului de "artă digitală". Demersul nu este simplu, având în vedere faptul ca mulți critici de artă contestă însăși existența artei digitale (deși nașterea sa se plasează în perioada anilor '60); ce nu a prins cu adevărat formă este contextul și un vocabular în care arta digitală să poată fi discutată și apreciată de către ne-practicieni în acest domeniu.

Datorită noutății și complexității fenomenului, există diferențe semnificative de opinie, atât în legătură cu definirea termenului de artă digitală, cât și în legătură cu existența și valoarea acestei noi forme de artă. Lipsa de adeziune la o definiție acceptată pe scară largă nu ține numai de noutatea și complexitatea fenomenului, ci și de perspectiva, de multe ori eronată, din care este analizat fenomenul.

Pentru a explica ce este "arta digitală", în contextul Legii române a dreptului de autor, este necesar să analizăm conceptul din perspectiva rolului artistului digital la realizarea lucrării supuse protecției legale. Care este, prin urmare, contribuția lui la realizarea acestei forme de artă și care este rolul mediului informatic (înțelegand prin acesta totalitatea mijloacelor informatice - echipamente și/sau programe informatice - puse la dispoziția artistului digital)?

Potrivit celei mai simple definiții, "arta digitală" este acea formă de artă realizată și aflată în formă digitală[260], stocată într-un mediu informatic.

---

259 Vezi o discutie detaliată în P. Samuelson, *The Digital Dilemma: Intellectual Property in the Information Age*, 28th Annual Telecommunications Policy Research Conference, 2000.

260 Termenul "digital" înseamnă binar, care vine din cuvântul englezesc *binary*, termen care, în sens larg, descrie tot ceea ce este lipsit de nuanțe de gri, adică tot ceea ce este alb sau negru, adevărat sau fals, cuplat sau decuplat. În sens strict, se referă la un sistem de numerație cu baza 2. În loc să fie exprimat în funcție de puteri ale lui 10, ca în sistemul zecimal, numărul este exprimat în funcție de puteri ale lui 2. Singurele cifre permise în acest sistem sunt 0 și 1. Acest sistem de numerație este foarte convenabil în descrierea circuitelor electronice, care sunt fie cuplate (adică, prin ele circulă curent electric), fie sunt decuplate (adică, nu circulă curent electric). A se vedea J. Browning, *Info & Tehnologie*, Ghid propus de The Economist Books, traducere din limba engleză de E. Bazac, Ed. Nemira, 52-53, 1999.

Considerăm că este deosebit de utilă clarificarea distincției dintre arta digitală și arta digitizată pentru evitarea confuziilor în interpretarea practică a textului de lege, confuzii ce pot interveni foarte ușor datorită considerării termenilor "digitală" și "digitizată" ca fiind similari.

Arta digitizată este, de fapt, artă stocată, accesată și vizualizată pe un calculator. Cum se arată într-o opinie, arta digitizată nu este artă "reală", ci reprezentarea digitală a acesteia[261]. Cele mai elocvente exemple de artă digitizată sunt muzeele și galeriile virtuale, care utilizează Web-ul în loc de săli de muzee sau galerii. Acest tip de artă începe să fie, datorită costului redus, a accesibilității deosbite, a reducerii distanțelor geografice, a inexistenței cozilor de la intrare ori a orelor stricte de vizitare, foarte agreat de iubitorii de artă din întreaga lume[262].

Un alt exemplu de artă digitizată este reprezentat de arhivele de imagini digitale asamblate de companii celebre, cum ar fi, spre exemplu, Getty Image (http://www.gettyimages.com/). Așadar, rolul mediului informatic în arta digitizată este acela de a oferi spațiu de stocare și expunere, iar cel al autorului de artă digitizată de a prelua opere de artă existente și de a le asambla și expune cu ajutorul mijloacelor digitale în "săli" de muzee virtuale, în galerii virtuale ori în arhive virtuale[263].

"Arta digitală" prezintă caracteristici care o fac diferită de "arta digitizată". Care sunt ingredientele cheie care asigură diferența dintre cele două forme de artă? În primul rând, trebuie punctat rolul artistului digital, care nu mai este un simplu "angajat" care asamblează, într-o anumită ordine sau poziție opere de artă existente în lumea reală; înarmat cu instrumente specifice tehnologii avansate [adică, programe informatice pentru artă (*art software*) și *hardware* specific (spre exemplu, monitoare CART, scannere etc.], în locul pensulelor sau paletelor de culori tradiționale, realizează noi opere de artă, care-și cer dreptul la recunoaștere artistică și la protecție legală. În al doilea rând, rolul calculatorului se schimbă: nu mai este un simplu mediu de stocare și expunere, ci un mijloc necesar în procesul creativ. Tocmai datorită caracteristicilor arătate mai sus, nu pot fi considerate opere de arta digitală datele sub formă de text, înregistrările audio sau video, în situația în care mediul informatic este utilizat în principal ca mediu de stocare.

Complexitatea domeniului face să se ridice întrebări legate de unele forme ale artei digitale, care au conotații juridice. Astfel, s-a pus întrebarea dacă este posibil să se realizeze unele forme de artă digitală de către calculator, fără să fie nevoie să intervină artistul digital?

Într-o opinie, s-a arătat că arta digitală nu este orice tip de artă creată de calculator, ci orice tip de artă realizată de un artist care utilizează anumite tipuri de tehnologii digitale[264]. În consecință, autorul mentionat exclude existența unor forme de artă digitală generate pur și simplu de calculator. În replică, însă, există

---

[261] A se vedea J. Miles și D. McLennan, *Digital goes critical*, accesibilă la http://www.artsjournal .com/artswatch/digitalcritical.htm.

[262] Spre exemplu, Muzeele Louvre (www.louvre.fr) sau Smithsonian (http://www.si.edu/), care atrag numeroși vizitatori pe site-ul Web.

[263] A se vedea, spre exemplu, Biblioteca Apostolica Vaticana (https://www.vatlib.it/), care conține reproduceri digitale a peste 4000 de manuscrise vechi

[264] A se vedea, T. Villot, *What is Digital Fine Art?*, 2002.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

specialişti care afirmă că există asemenea forme, şi exemplul cel mai sugestiv prezentat în argumentaţie sunt *fractalii*[265].

Din exprimarea de mai sus, nu trebuie să se înţeleagă că ar exista forme de artă digitală fără autor. În acest caz, dreptul de autor îl are persoana care a scris algoritmul aflat la baza programului informatic. Simpla rulare a programului informatic duce la vizualizarea fractalilor, tocmai de aceea există opinia că în acest caz avem de-a face cu o operă de artă generată pur şi simplu de calculator, utilizatorul neavând nici un rol creator, prin urmare neputând cere protecţie pentru autor. Autorul programului informatic va putea opta, în funcţie de interesele sale şi de posibilităţile oferite de legislaţia naţională, fie pentru protectia programelor informatice în formele existente, fie pentru protecţia oferită operelor de artă digitală.

Considerăm deosebit de utilă, pentru înţelegerea profundă a conceptului de operă de artă digitală, prezentarea formelor sub care se prezintă actualmente arta digitală. Varietatea extraordinară a mijloacelor puse la dispoziţie de mediul informatic artiştilor digitali a dus la apariţia a numeroase forme de artă digitală, dintre care enumeram în continuare pe cele mai frecvente: fotografia digitală, ilustraţia digitală, efecte speciale digitale utilizate în industria cinematografică, grafice digitale, imagini digitale, muzică digitală, design pentru jocuri video digitale.

Este important de reţinut faptul că, deşi arta electronică este considerată de mulţi sinonimă cu arta digitală, în realitate relaţia dintre ele este asemănătoare cu cea dintre semnatura electronică şi cea digitală; prin urmare, arta electronică are un înteles mai larg, cuprinzând arta digitală şi, pe lângă aceasta, o mulţime de alte produse rezultate din inter-relaţiile cu arta clasică, cum ar fi, spre exemplu, arta digitizată, de care am amintit mai sus.

Frecvenţa cu care sunt utilizate tipurile de arta digitala pe care le-am prezentat mai sus, precum şi altele, demonstrează că arta digitală merită includerea în categoria de "artă serioasă", alături de arta clasică. Spre exemplu, mass-media din zilele noastre utilizează în cantităţi însemnate arta digitală sub forma reclamelor, iar calculatoarele sunt folosite extensiv pentru a crea efecte speciale.

Un tip de opere de artă digitală mult apreciat în zilele noastre este reprezentat de graficele tridimensionale, create printr-un proces digital elaborat, de îmbinare a unor forme geometrice, rezultând, în final, forme digitale tridimensionale care dau impresia că sunt reale, obiecte şi scene, utilizate în produse media variate cum ar fi filme, televiziune, alte efecte speciale.

Calculatoarele sunt azi folosite cu succes la crearea muzicii electronice, iar autorilor acestora li se recunoaşte nu numai meritul, ci şi dreptul de proprietate intelectuală. Disponibilitatea programelor informatice speciale utilizate în tehnicile de prelucrare a fotografiei a dat nastere unor biblioteci creative imense de imagini modificate la un asemenea nivel că nu mai exista nici urmă de asemănare cu imaginile de origine.

---

265 Fractalul reprezintă o formă, de multe ori desenata pe calculator, care se repetă pe ea însăşi într-un pattern, în mod continuu; frumuseţea irezistibilă este dată tocmai de dispunerea acestor forme în mediul informatic.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

Utilizând versiunile electronice ale pensulelor și creioanelor tradiționale, filtre și dispozitive digitale de mărire și modificare a imaginilor, fotografii digitali au creat "neografii", adică forme avansate ale imaginilor clasice, la dimensiuni de neimaginat în condițiile utilizării mijloacelor fotografice clasice. În plus, artiștii digitali pot manipula picturi, imagini, colaje, litografii, pot combina la infinit forme de arta și metode. În acest context, este important să menționăm că toate acestea pot duce cu ușurință la încălcarea drepturilor altor creatori de opere de arta, fie ele digitale sau traditionale. Mediul digital, caracterizat printr-un caracter cameleonic accentuat, are nevoie de legi noi, inclusiv în domeniul proprietății intelectuale, care să răspundă specificului său tehnic, ce scapă persoanelor care nu au pregătire în domeniul tehnologiilor informației.

Neînțelegerea acestui tip special de artă, neacordarea protecției legale specifice, precum și abuzurile celor care se consideră creatori de opere de artă digitală, deși în realitate nu este așa, a dus la acțiuni în justiție[266]. Acesta este un semnal de alarmă atât pentru legiutor, cât și pentru cei ce au interese în acest domeniu, de a lua măsuri de clarificare a noilor forme de creații intelectuale care au luat naștere din îngemănarea artei cu tehnologia, de a prevedea măsuri de protecție a acestora, dar și de a apăra drepturile autorilor operelor de artă tradițională, care pot fi lezate de mijloacele noi puse la dispoziție de mediul digital (a se vedea, spre exemplu, cazuri de *grafitti virtual*, prin care, cu ajutorul unui program informatic special, au fost "mutilate", prin adăugare, ștergere etc., opere clasice celebre).

3.2.3 Încălcarea drepturilor privind conținutul digital protejat

Capacitatea persoanelor fizice și juridice de a accesa conținut digital pe Internet este esențială pentru progresul economic și evoluția mediului informatic[267]. Dezvoltarea tehnologică a multiplicat și diversificat vectorii de creație, producție și exploatare, dar a creat și numeroase modalități de încălcare a drepturilor de proprietate intelectuală. Produsele digitale sunt foarte ușor de reprodus, la o calitate identică sau foarte apropiată de produsul original, distribuirea fiind extrem de facilă în mediul digital, la un cost marginal sau, în unele cazuri, chiar zero, evitând orice taxe sau tarife vamale[268], ceea ce le face

---

[266] Cazuri interesante sunt, spre exemplu, Barbie și Star Trek: s-a pus problema dacă artiștii digitali au încălcat drepturile de proprietate intelectuală deținute de creatorii operelor originale prin distorsionarea imaginilor originale (Barbie și Star Trek), sau sunt îndreptățiți să ceară drepturi de autor pentru operele digitale rezultate prin modificarea operelor originale; a se vedea, în același sens, articolul lui R. Winick *Intelectual property, defamation and the digital alteration of visual images*, 21 Column, 1997.

[267] Vezi, spre exemplu, B. van Schewick, *Network neutrality nuances*, Communications Of The ACM, February, Vol. 52, No. 2, 2009.

[268] Vezi o discuție extinsă în OECD, *Piracy of digital content*, 2009.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

extreme de vulnerabile la încălcarea drepturilor de proprietate intelectuală[269]. Pirateria digitală, în special pe Internet[270], este o amenințare deosebită pentru drepturile titularilor și pentru securitatea economică a statelor.

Infracțiunile din domeniul proprietății intelectuale au întotdeauna o victimă directă – deținătorul drepturilor – și, adițional fraudei executate în detrimentul receptorului produselor digitale piratate, subminează întregul sistem al proprietății intelectuale. În general, se consideră că pirateria digitală este chiar mai "productivă" pentru cei care o comit decât comerțul ilegal cu droguri[271]. Astfel, copii ilicite ale programelor informatice, spre exemplu, pot genera un profit de 900%[272]. Deoarece acest tip de infracțiuni poate fi comis fără un contact direct cu victima, aceasta din urmă este, cel mai adesea, fără apărare în aceste situații. Combaterea efectivă a acestui tip de piraterie, în special în forma sa de comitere pe Internet, este esențială pentru dezvoltarea economiei digitale[273].

Încălcarea acestor drepturi reprezintă un fenomen îngrijorător prin dimensiunile sale internaționale, prin potențialul de a cauza pierderi masive titularilor drepturilor și economiilor naționale și prin problemele pe care le ridică privind protecția consumatorilor. Există numeroase utilitare care permit încălcarea drepturilor titularilor[274], iar folosirea Internetului face posibilă distribuirea de produse piratate în formă digitală, în câteva secunde, oriunde pe glob. Mai mult, acest fenomen pare a fi din ce în ce mai legat de crima organizată[275].

Încălcarea drepturilor de autor se poate petrece prin achiziționare sau folosire neautorizată și poate afecta categorii largi de lucrări protejabile (*inter alia*): lucrări literare (cărți, articole, programe informatice, compilații de informații, baze de date) lucrări muzicale, înregistrări audio, filme etc.). Conținutul digital este o componentă importantă în industria tehnologiilor informației și comunicației[276], noi tipuri de conținut fiind dezvoltate (spre exemplu, jocuri online) și noi modele de afaceri, incluzând cele de tip abonament sau *pay-per-use* (mai ales în cazul muzicii).

---

269 Vezi, spre exemplu, R. Dokhanchy, *Cooperative infringement: I get by (infringement laws) with a little help from my friends*, Berkeley Technology Law Journal, Vol. 26 (2011); W. Carroll, *I Want my MP3: Secondary Copyright Liability in a Hidden Peer-to-Peer Network*, 5 Journal of High Technology Law 235, 2005.

270 Vezi W. D. Gunter, *Internet Scallywags: A Comparative Analysis of Multiple Forms and Measurements of Digital Piracy*, Western Criminology Review 10(1), 15-28, 2009.

271 Vezi Union des Fabricants, *Counterfeiting & Organised Crime Report*, 2nd Ed., 2004.

272 Vezi Ioana Vasiu și Lucian Vasiu, *Protecția programelor informatice: Aspecte tehnice și legale*, Revista Română de Dreptul Proprietății Intelectuale, Anul V, Nr. 1 (14), 27-33, 2008.

273 Vezi D. Goldstone, *Deciding Whether to Prosecute an Intellectual Property Case*, USA Bulletin, 2001.

274 Numeroase țări au adoptat legi care fac ilegală încălcarea măsurilor de protecție instituite de deținătorii drepturilor pentru protecția lucrărilor lor (spre exemplu, în SUA, the *Digital Millennium Copyright Act* din 1998 (DMCA)). Cu toate acestea, utilitare care încalcă asemenea măsuri sunt prezente – vezi FairUse4WM în B. Ortega, *NewsBriefs*, IEEE Security & Privacy, 6, 2006.

275 Vezi Commission of the European Communities, *Amended proposal for a Directive of the European Parliament and of the Council on criminal measures aimed at ensuring the enforcement of intellectual property rights*, Brussels, 2006.

276 Vezi OECD, *Information Technology Outlook*, 2010.

Problemele majore asociate cu încălcarea drepturilor de proprietate intelectuală în mediul digital, în particular în cazul site-urilor cu conținut generat de utilizator[277], se referă la cantitatea masivă de conținut protejat care este plasată și transmisă digital și de problemele ridicate de licențierea drepturilor la o asemenea scară. Problema protejării drepturilor de proprietate intelectuală, în acest mediu, este complicată de faptul că, în unele situații, putem vorbi de tolerarea explicită a unei copieri limitate (spre exemplu, the Recording Industry Association of America în *Piracy: Online and On the Street* acceptă o copiere limitată[278], cu scopul de utilizare la nivel personal, dar nu aprobă distribuirea de conținut digital protejat online) și la dificultatea determinării cu precizie a existenței încălcărilor drepturilor de proprietate intelectuală[279].

Preocuparea la nivel UE privind drepturile de autor este relevată de un număr de Directive[280]. O întrebare esențială, în acest context, privește modul de abordare: realizarea unui nou sistem de legi care să adreseze acest tip de mediu sau modificarea regimului existent astfel încât acesta să adreseze problemele ridicate de mediul digital[281]. Considerăm că doar o abordare holistică, implicând o legislație efectivă și participarea activă a deținătorilor și distribuitorilor de conținut digital poate avea un impact pozitiv în încercarea de protejarea a drepturilor de proprietate intelectuală în acest mediu[282]. Adițional, administratorii site-urilor cu conținut generat de utilizatori trebuie să adreseze problemele ridicate de licențierea produselor digitale protejate prin drept de autor, să includă programe de educare în domeniul protejării acestor drepturi, să dezvolte proceduri de management al riscului ridicat de posibilele încălcări ale drepturilor de autor și să creeze mecanisme prin care personalul implicat să fie capabil să depisteze și să adreseze problemele ridicate de acest mediu.

Categoriile de lucrări care sunt acoperite prin drept de autor și care sunt foarte expuse pirateriei digitale includ filme, programe informatice, înregistrări muzicale și coreografice, programe de televiziune etc. Printre provocările deosebite cu care se confruntă combaterea pirateriei digitale pe Internet, se numără[283]:

- Locațiile piraților digitali pe Internet sunt dificil de detectat;
- Calcularea daunelor și pierderilor este foarte dificilă, deoarece este greu să fie determinat numărul de copii ilegale realizate/distribuite;

277 Vezi Ioana Vasiu și Lucian Vasiu, *We Create, You Tube, They Infringe*, op. cit.

278 Vezi și Tim Wu, *Tolerated use*, 31 Columbia Journal of Law & the Arts, 619-20, 2008.

279 Vezi, spre exemplu, cazul *Rossi v. Motion Picture Association of America*, în care s-a solicitat închiderea site-ului www.internetmovies.com, care oferea utilizatorilor posibilitatea de a descărca filme într-o manieră care încalcă drepturile de proprietate intelectuală, discutat în Berkeley Technology Law Journal, *Rossi v. Motion Picture Association of America Inc.*, 21 Berkeley Technology Law Journal, 399 (2006).

280 Vezi Directivele Parlamentului European 2001/29/EC, 2006/115/EC și 2006/116/EC.

281 A se vedea o discuție extinsă în *The principles for user generated content services: a middle-ground approach to cyber-governance*, Harvard Law Review, Vol. 121, 1387, 2008.

282 Vezi, spre exemplu, http://www.ugcprinciples.com.

283 Vezi o discuție pe această temă la locația http://www.house.gov/judiciary/digr0512.htm (accesată 8 octombrie 2008).

- Nici o agenţie guvernamentală nu are ca responsabilitate primară combaterea infracţiunilor realizate pe Internet;
- Aspecte jurisdicţionale;
- Investigatorii calificaţi în acest domeniu sunt rari şi dificil de păstrat.

Protecţia drepturilor de proprietate intelectuală este esenţială pentru promovarea inovaţiei şi a creativităţii, pentru realizarea de produse de calitate şi pentru dezvoltare economică. Ca răspuns la aceste fenomen sofisticat şi periculos, au fost elaborate instrumente juridice şi au fost întărite capacităţile de investigare. Pentru apărarea drepturilor de autor sau a mărcilor există un număr de instrumente internaţionale[284] (spre exemplu, *Charter of Fundamental Rights* (articolul 17.2); Convenţiile de la Berna, Brussels şi Paris; WIPO *Copyright Treaty* şi *Performances and Phonograms Treaty*; World Trade Organisation *Agreement on trade-related aspects of intellectual property rights*) şi legi naţionale[285]. În SUA, protecţia drepturilor de autor şi a mărcilor de comerţ are o importanţă deosebită, paradigma îmbrăţişată de Congres făcând infracţiunile din domeniul dreptului de autor similare furtului din spaţiul fizic[286].

La nivelul Uniunii Europene, pentru a se alinia la instrumentele internaţionale la care este parte, în martie 2004 a fost adoptată Directiva *on the Enforcement of Intellectual Property Rights* (numită şi *IPR Enforcement Directive*). Directiva urmăreşte consolidarea legislaţiei ţărilor membre în domeniul respectării drepturilor de proprietate intelectuală (măsurile din domeniu trebuie să fie efective, proporţionate şi disuasive, fără a acţiona ca o barieră a comerţului) şi acordarea autorităţilor naţionale de puteri crescute de urmărire a infractorilor şi obţinerea de compensaţii pentru deţinătorii drepturilor. Conform articolului 3(1), statele membre vor fi cenzurate în European Court of Justice dacă procedurilor lor civile privind încălcarea drepturilor de proprietate intelectuală sunt prea complicate sau costisitoare, sau dacă implică limite de timp nerezonabile.

În octombrie 2006, Consiliul pentru Justiţie şi Afaceri Interne (*Justice and Home Affairs Council*) a discutat amendamente ale Comisiei Europene subliniind principiul subsidiarităţii. Pentru investigarea infracţiunilor de piraterie digitală au fost create organisme speciale, cum ar fi *INTERPOL Intellectual Property Crime Action Group* (IIPCAG), *Rapid Enforcement Allied Computer Team* (REACT) Task Force sau *Computer and Technology Crime High-Tech Response Team* (CATCH). Pentru a ilustra diverse aspecte importante ale acestui fenomen (magnitutidinea şi sofisticarea fenomenului, dificultăţile investigării acestor

---

284 Vezi C. R. Romiţan, *Protecţia penală a proprietăţii intelectuale*, Ed. C. H. Beck, 2006.

285 Vezi, pentru România, C. R. Romiţan, *Creaţii intelectuale, proprietate intelectuală sau drept de autor*, Revista Română de Dreptul Proprietăţii Intelectuale, V, 2 (15), 98-108, 2008.

286 Vezi, spre exemplu, citate cum ar fi "*Just as we will not tolerate the theft of software, CDs, books, or movie cassettes from a store, so we will not permit the stealing of intellectual property over the Internet*"; "*[p]irating works online is the same as shoplifting a videotape, book or record from a store*" în E. Goldman, *A Road to No Warez: The No Electronic Theft Act and Criminal Copyright Infringement*, Oregon Law Review, Vol. 82, 2003. Vezi, spre exemplu, US DoJ, *Progress Report of the department of justice's Task force on intellectual property*, 2006.

infracţiuni, aspecte privind încălcarea unor drepturi civile, aspecte jurisdicţionale etc.), prezentăm un număr de cazuri relevante.

Mediaset/YouTube[287]

Firma italiană Mediaset, controlată de familia primului ministru Silvio Berlusconi, a pornit o acţiune judiciară împotriva companiei Google şi a unităţii sale YouTube, în care solicită cel puţin 500 milioane euro pentru folosirea ilegală de materiale ale Mediaset. Conform estimărilor Mediaset, cel puţin 4.643 video-uri şi clip-uri care îi aparţin, echivalentul a peste 325 ore de transmisie fără drept au fost implicate.

Pirates with Attitudes

Pirates With Attitude (PWA) a fost o locaţie de tip warez[288], care opera 13 servere FTP pentru încărcarea şi descărcarea de programe informatice. Pe parcursul operaţiunilor ilegale, peste 30.000 de programe informatice (jocuri, fişiere muzicale în format MP3, sisteme de operare, programe utilitare, programe aplicaţii de la firme cum ar fi Microsoft, Adobe, Norton, Oracle, Lotus sau Novell) au fost încărcate pe serverele grupului şi descărcate de peste 100 de indivizi. Un număr de 17 persoane au fost condamnate în acest caz, 12 fiind membrii PWA, 5 fiind angajaţi Intel Corp., care au furnizat echipament pentru operaţiunile PWA[289].

Laney & Grace[290]

S. Laney şi T. Grace au vândut programe informatice Microsoft cu licenţe frauduloase. Unele programe erau original marcate "*Academic Edition - Not for Resale*", în timp ce altele erau marcate "*Original Equipment Manufacture* (OEM)"[291]. Programele informatice au fost obţinute de către cei doi indivizi la preţuri mult sub cele practicate pentru vânzări *en gross* sau *en detail*.

Licenţele şi marcajele produselor au fost alterate pentru a prea a fi produse standard, după care au fost vândute la preţuri apropiate de cele practicate de retaileri. Adiţional, cei doi au alterat licenţe pentru programe informatice server să autorizeze un număr mai mare de utilizatori decât cel setat iniţial şi le-au revândut la preţuri substanţial mai mari.

Unele dintre programele achiziţionate şi revândute de cei doi proveneau de la angajaţi Microsoft care au exploatat o eroare internă în sistemul de comenzi al firmei (aceşti au fost de asemenea condamnaţi penal pentru activităţile lor ilegale). Infractorii au admis că au vândut astfel produse de circa 20 milioane USD şi au fost

---

287 Vezi o prezentare pe larg a cazului la locaţia http://www.informationweek.com/news /internet/google/showArticle.jhtml?articleID=209900317 (accesată 8 octombrie 2008).

288 "Warez" este prescurtare de la "software", cu "z" folosit ca o convenţie de numire a lucrărilor piratate.

289 În acest caz au furnizat asistenţă şi Business Software Alliance şi Software and Information Industry Association.

290 Vezi prezentarea cazului la locaţia http://www.cybercrime.gov/laneySent.htm (accesată 8 octombrie 2008).

291 Pentru detalii privind licenţele de tip OEM, a se vedea I. Vasiu şi L. Vasiu, *Informatică juridică şi Drept Informatic 2009*, Ed. Albastră, Cluj-Napoca, 2009.

BCU CLUJ / CENTRAL UNIVERSITY LIBRARY

condamnaţi la 5 ani închisoare, 3 ani eliberare supervizată şi peste 9 milioane de USD restituiri (conform *Conspiracy to Traffic in Counterfeit Labels and Computer Program Documentation* şi *Conspiracy to Engage in Money Laundering*).

Peterson[292]

Între 2003 şi 2005, N. L. Peterson a administrat locaţia web <www.ibackups.net>, prin intermediul căreia a vândut copii ilegale ale programelor informatice produse de Adobe Systems, Inc., Macromedia Inc., Microsoft Corporation, Sonic Solutions şi Symantec Corporation, la preţuri mult sub cele de retail (copiile erau distribuite electronic sau prin transmiterea prin poşta a unui CD conţinând programul informatic). Peterson a fost condamnat la 7 ani închisoare şi obligat să plătească restituiri de peste 5 milioane USD.

D-Elite[293]

S. R. McCausland a fost implicat în reţeaua BitTorrent, reţea de tip P2P[294] cunoscută anterior sub numele de Elite Torrents, investigat şi condamnat. Investigaţia acestui caz a făcut parte din *Operation D-Elite*, o operaţiune federală împotriva furnizorilor de lucrări piratate către reţeaua Elite Torrents, care la un moment dat atrăgea peste 133.000 de membri şi facilita distribuirea ilegală a peste 2 milioane de copii de filme, muzică, programe şi jocuri informatice, unele dintre aceste lucrări fiind disponibile chiar înainte de a fi puse în vânzare sau a fi proiectate în săli de cinema (spre exemplu, Star Wars Episode III: Revenge of the Sith, a fost disponibil cu peste 6 săptămâni înainte de a fi proiectat în săli de cinema).

Hardick[295]

R. Hardick a participat la scheme de tip "warez", în care anumiţi participanţi numiţi "furnizori" obţin acces la lucrări protejate prin drept de autor (programe informatice, jocuri video, filme, muzică), alţi participanţi numiţi "spărgători" (*crackers*) îşi folosesc cunoştinţele tehnice pentru a "ocoli", invalida sau "sparge" protecţia conţinutul digital, iar alţii numiţi "curieri" distribuie conţinutul piratat către diverse locaţii de stocare (locaţii FTP) pe Internet pentru a fi accesate de către alţii. Hardick a lansat şi întreţinut o locaţie FTP numită "The Boxer Rebellion" (TBR) pe care a încărcat peste 62000 de fişiere.

---

292 Vezi prezentarea cazului la locaţia http://www.cybercrime.gov/petersonSent.htm (accesată 8 octombrie 2008).

293 Vezi prezentarea cazului la locaţia http://www.cybercrime.gov/mccauslandPlea.htm (accesată 8 octombrie 2008).

294 O reţea P2P sau *Peer to Peer network* este o "clasă de aplicaţii care exploatează resursele de stocare, conţinut sau cele umane" disponibile la "marginea" Internetului. Exemple de astfel de reţele sunt servici ca Napster, Gnutella, LimeWire, Morpheus, Kaaza, Bit Torrent sau proiecte de cercetare cum este UC Berkeley Seti@home. Ceea ce caracterizează permit schimbul de fişiere fără a depinde de un server care să coordoneze procesul; nu există un loc central unde să se afle date ci un număr de sisteme care partajează date informatice.

295 Vezi prezentarea cazului la locaţia http://www.cybercrime.gov (accesată 8 octombrie 2008).

B.C.U. „M. EMINESCU" IAŞI

BCU IASI / CENTRAL UNIVERSITY LIBRARY

PirateBay[296]

Într-o investigaţie pornită de procurori din Bergamo, în 1 august 2008, a fost emis un ordin al justiţiei italiene care solicita "confiscarea" locaţiei web PirateBay, găzduită în afara Italiei, pentru afişarea unei colecţii de legături (*links*) către materiale duplicate ilegal. Ordinul a fost implementat în 10 august 2008 prin forţarea furnizorilor italieni de servicii Internet să blocheze accesul la respectiva locaţie, atât la numele de domeniu, cât şi la numărul IP asociat. Deţinătorii PirateBay au reacţionat prompt şi au schimbat numărul IP şi numele locaţiei în <labaia.org> ("La Baia" înseamnă, în limba italiană, "The Bay"), promovând şi măsuri de trecere peste măsura de blocare luată de autorităţi (au solicitat schimbarea DNS to OpenDNS, pentru a putea trece de filtrele furnizorilor de servicii Internet).

Utilizatorii care încercau să acceseze locaţia "confiscată" erau redirectaţi ctre un număr IP asociat unor servere localizate într-o altă ţară, aparţinând unei asociaţii care protejează drepturile de proprietate intelectuală. Acest lucru permite unei asociaţii private, aflate în afara jurisdicţiei italiene, să colecteze date privind traficul Internet, date care, asociate cu cele ale furnizorului italian de servicii Internet, permit identificarea şi posibila investigare penală a unor terţe părţi care nu sunt implicate în cazul anchetat la Bergamo, ceea ce ridică serioase întrebări privind respectarea unor drepturi civile şi unele aspecte jurisdicţionale sau procedurale[297].

Buccaneer[298]

Operaţiunea Buccaneer a ţintit grupuri de tip "warez" şi a implicat mandate de căutare în mai multe ţări. În principal, a fost vizat DrinkOrDie, unul dintre cele mai vechi şi cunoscute grupuri de tip "warez", fondat în Moscova în 1993, cu extindere globală subsecvent[299], dar şi altele asemenea grupuri, cum ar fi Razor1911, RiSCISO, MYTH, POPZ, RequestToSend (RTS), WeLoveWarez (WLW) şi RiSC.131. Arhivele grupului DrinkOrDie conţineau 2 teraocteţi de programe informatice piratate, cu o valoare estimată de multe milioane de USD.

3.2.4 Managementul digital al drepturilor de autor

Caracterul sistemului proprietăţii intelectuale este evoluţionar, în timp ce natura drepturilor (controlul şi exploatarea) rămâne relativ constantă, maniera în care acestea sunt exprimate se adaptează constant la dezvoltările tehnologice[300].

---

296 Vezi detalii la locaţia http://www.edri.org/edrigram/number6.16/italy-blocks-piratebay (accesată 8 octombrie 2008).

297 Vezi http://edri.blogactiv.eu/2008/10/09/an-update-on-the-italian-piratebay-case/ (accesată 8 octombrie 2008).

298 Vezi U.S. DoJ, *Multiple Enforcement Actions Worldwide Snare Top "Warez" Leadership*, 2001, la locaţia http://www.justice.gov/archive/opa/pr/2001/December/01_crm_643.htm.

299 Printre alte "realizări", grupul ar fi făcut disponibil sistemul de operare Microsoft Windows 95 cu 2 săptămâni înainte de lansarea comercială.

300 Vezi o discuţie extinsă pe această temă în WIPO, *Intellectual property on the Internet: A survey of issues*, 2002.

Pentru protejarea creațiilor posibilă prin *măsuri* tehnologice; acestea sunt definite de Directiva 2001/29/CE[301] ca fiind orice tehnologie, dispozitiv sau componentă care, în cursul funcționării normale, este proiectată pentru a preveni sau limita acțiuni asupra lucrărilor sau altor obiecte protejate care nu sunt autorizate de titularul de drepturi de autor și de alte drepturi conexe conform prevederilor legale, sau de titularul dreptului sui generis prevăzut la capitolul III din Directiva 96/9/CE. Principalele măsuri tehnice cuprind protecția prin parolă, folosirea de chei fizice (*dongles*), criptare, codare regională (care impiedica folosirea DVD-urilor în afara zonei programate), protecție online a filmelor închiriate, protocol care permite transmiterea de muzică doar către aplicația utilizatorului care nu permite copierea (*secret handshake protocol*), marcarea prin semne speciale[302].

Sistemele DRM pot proteja materiale în format digital printr-o combinație de măsuri: criptare, marcare digitală cu informații care identifică titularul dreoturilor și condițiile de folosire. Esențial în cazul tuturor sistemelor DRM este nevoia de drepturi digitale - drepturi de reproducere și diseminare a materialului în formă digitală. Deținătorii dreptului pot exercita oricare dintre drepturile lor exclusive sau pot acorda permisiune altora să o facă (prin licențiere).

Măsurile tehnologice sunt considerate eficiente când folosirea unei lucrări sau a unui alt obiect protejat este controlată de către titularii de drepturi în baza aplicării unui cod de acces sau a unui proces de protecție, cum ar fi criptarea, bruierea sau alte transformări ale lucrării sau ale altui obiect protejat, sau a unui mecanism de control al copierii, care atinge obiectivele protecției. Sistemele de management digital al drepturilor (*Digital rights management systems - DRM systems*) și legile care fac ilegală circumvenția acestor sisteme[303] ocupă un loc important în încercarea de a impune respectarea drepturilor de proprietate intelectuală. Sistemele DRM promit să împiedice încălcarea conținutului digital prin controlarea drepturilor de reproducție[304] (reproducție temporară, cum ar fi o copie în memoria unui calculator, sau copii permanente, stocate pe discuri) și comunicare.

Sistemele DRM promit să ofere o modalitate sigură de distribuire a conținutului digital și 'a află la întretăierea dintre considerații tehnice, legale și comerciale[305]. Principalul scop al sistemelor DRM este respectarea licențelor de

---

301 Vezi Directiva Parlamentului European și a Consiliului 2001/29/CE din 22 mai 2001 de armonizare a anumitor aspecte privind dreptul de autor și drepturile conexe în societatea informațională.

302 Vezi R. Iwahashi, *How to circumvent technological protection measures without violating the DMCA: An examination of technological protection measures under current legal standards*, Berkeley Technology Law Journal, Vol. 26, 2011.

303 Vezi, spre exemplu, J. C. Fernández-Molina, *Laws against the Circumvention of Copyright Technological Protection*, Journal of Documentation, 59 (1), 41-68, 2003.

304 Vezi P. Samuelson și J. Schultz, *Should copyright owners have to give notice of their use of technical protection measures?*, Journal. On Telecommunications & High Technology Law, Vol. 6, 41-75, 2007; A. Sundararajan, *Managing Digital Piracy: Pricing and Protection*, Information Systems Research, Vol. 15, No. 3, September, 287–308, 2004.

305 Vezi P. Samuelson, *Digital Rights Management {and, or, vs.} the Law*, Communications of the ACM (2003). Exemple de sisteme DRM sunt Adobe Adept DRM, Apple FairPlay,

folosire a obiectelor protejate și definirea regulilor privind folosirea autorizată[306]. Sistemele DRM sunt asimilabile controlului de tip mandatar (*Mandatory Access Control*), cu o politică de folosire centrală, setată de un administrator și impusă de programe informatice incorporate în sistemul de operare, echipament sau în ambele. Sistemele DRM pot incorpora și mecanisme care să răspundă activ la încălcări ale securității, cum ar fi filtre specializate, impresiuni audio și alte tehnici care împiedică accesul la conținut digital piratat.

Capacitatea de a modifica politicile de folosire după ce un document este distribuit este una dintre posibilitățile oferite de sistemele DRM. Sistemele DRM avansate pormit unui document protejat să contacteze un server pentru a autentifica un utilizator și a verifica permisiunile la fiecare accesare a respectivului document. Asemenea sisteme pot, de asemenea, să blocheze permisiunile în mod automat și să înregistreze utilizatorii și acțiunile pe care aceștia le încearcă asupra documentului protejat.

Susținătorii acestor sisteme argumentează că fără aceste sisteme și legile aferente nu este posibilă protecția efectivă a dreptului de autor în mediul digital și văd aceste sisteme ca o modalitate de adresare a descrierii, identificării, comercializării, protejării și monitorizării modului de folosire a obiectelor protejate, inclusiv managementul relației cu deținătorii drepturilor. Protecția conținutului digital într-un sistem DRM se bazează pe diverse modalități: protecție prin tehnologie cu suport legislativ; protecție prin contracte cu protecție oferită de tehnologie și reglementări anti-circumvenție; protecție prin licențe tehnologice.

Pentru a facilita comercializarea conținutului digital și a drepturilor asociate, sistemele DRM folosesc *metadata* pentru a descrie formal conținutul digital și parametrii asociați: sistemele metadata folosesc standarde care permit descroerea conținutului digital (spre exemplu, DOI, ISBN, ISRC, ISWC și PII), deținătorii drepturilor (spre exemplu CAE/IPI) și termenii de folosire asociați (adică, "regulile de folosire", definite în limbaje de management a drepturilor, cum ar fi XrML sau ODRL). Standarde DRM importante includ *the Content Protection for Recordable and Prerecorded Media* (CPRM/CPPM), *the Digital Transmission Content Protection* și *the High-bandwidth Digital Content Protection*[307].

Oponenții acestor sisteme argumentează că asemenea sisteme și legi modifică balanța normală dintre drepturi și limitări, și afectează aspecte importante, cum ar fi aspecte privind libertatea de expresie sau legi antitrust[308].

Mobipocket, Microsoft Reader, SecuRom, Apple *iPod* (muzica pentru iPod se poate cumpăra doar folosind iTunes Store), LockLizard etc.

306 Vezi S. Haber, B. Horne, J. Pato, T. Sander, R. E. Tarjan, *If Piracy is the Problem, Is DRM the Answer?*, 2003; C. Sprigman, *"LOCKWARE": The Promise And Peril Of Hollywood's Intellectual Property Strategy For The Digital Age*, 2002.

307 Vezi detalii în S. Bechtold, *From Copyright to Information Law - Implications of Digital Rights Management*, 2002; B. Rosenblatt, B. Trippe, S. Mooney, *Digital Rights Management: Business and Technology*, 2001.

308 Vezi, spre exemplu, A. Matin, *Digital rights management (DRM) in online music stores*, Loyola Of Los Angeles Entertainment Law Review, Vol. 28, 2009; D. L. Burk, J. E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, Harvard Journal of Law and Technology, 15, 2001; S. Leisten, T. Flew, G. Hearn, *Alternative Intellectual Property Systems*

Mai mult, se poate argumenta că asemenea sisteme invadează spaţiul electronic al altor entităţi şi pot cauza probleme semnificative calculatoarelor acestora.

Într-un astfel de caz, CD-uri Sony BMG Entertainment, cu măsuri DRM realizate pentru a forţa utilizatorii Windows să asculte piese folosind doar o anumită versiune de Media Player. Ascultarea acestor CD-uri rezultă în instalarea de cod special care restricţionează numărul de copii care poate fi realizat, dar care crează şi structuri de directori clandestine cu fişiere ascunse. Încercarea de a înlătura aceste fişiere sau de a şterge directorii astfel instalaţi a rezultat în daune semnificative cauzate sistemelor sau datelor informatice. Deoarece codul Sony încalcă numeroase legi prin aceea că dăunează sistemelor şi acţionează de o manieră maliţioasă, au urmat complicaţii legale[309]. Un alt caz de încălcare a securităţii şi intimităţii este oferit de programul Adobe pentru e-book "Digital Editions", care înregistrează fiecare documenta adăugat de utilizatori "librăriei" lor şi transmite aceste fişiere log către dezvoltator[310].

Statutul legal al sistemelor DRM este recunoscut formal în numeroase ţări care au semnat *WIPO Copyright Treaty*[311]. Acest Tratat stabileşte mai multe norme de aplicare a legilor din domeniul dreptului de autor în mediul digital (*inter alia*):

- Deţinătorul drepturilor trebuie să aibă dreptul exclusiv de a controla realizarea de copii ale lucrărilor în formă digitală;
- Deţinătorul drepturilor trebuie să aibă dreptul exclusiv de a controla comunicarea publică a lucrărilor;
- Excepţii şi limitări cum ar fi folosirea legitimă[312] pot fi menţinute şi pot fi create chiar noi excepţii şi limitări, adecvate mediului digital;
- Este ilegală modificarea informaţiei de management a drepturilor în măsura în care o asemenea acţiune ar facilita încălcarea drepturilor în mediul digital;
- Necesitatea remediilor legale împotriva circumvenţiei măsurilor tehnologice folosite de deţinătorii drepturilor pentru protejarea lucrărilor lor.

---

for the Digital Age, 2005; R. C. Shah, J. P. Kesan, *Manipulating the governance characteristics of code* (2003); GNU Project, *Confusing words and phrases that are worth avoiding*, 2002.

309 Vezi J. A. Halderman şi E. W. Felten, *Lessons from the Sony CD DRM Episode*, 15th USENIX Security Symposium, 2006) şi J. E. Cohen, *DRM and Privacy*, Communications of the ACM, 46 (4), 47-49, 2003.

310 Vezi *Adobe Spyware Reveals (Again) the Price of DRM: Your Privacy and Security*, https://www.eff.org/deeplinks/2014/10/adobe-spyware-reveals-again-price-drm-your-privacy-and-security.

311 Vezi *the WIPO Copyright Treaty* la http://www.wipo.int/treaties/ip/wct/index.html (în vigoare din 6 martie 2002).

312 Vezi T. K. Armstrong, *Digital rights management and the process of fair use*, Harvard Journal of Law & Technology, Vol. 20, No. 1, Fall, 49-121, 2006.

Există mai multe modele care permit titularilor drepturilor controlul asupra folosiri produselor lor[313]:

- *Model I*: Acest model permite titularului drepturilor controlul accesului prin folosirea de parole ca unică facilitate DRM; conținutul nu este criptat, iar acest model nu controlează copierea sau redistribuirea.
- *Model II*: Acest model permite titularului drepturilor controlul accesului, copierii și redistribuirii. Controlul este realizat prin criptare, care restricționează accesul și ce se poate face cu aceste materiale. Programe informatice speciale, furnizate de titularul drepturilor sau în numele acestuia, sunt necesare pentru a obține acces la materialul criptat.
- *Model III*: Acest model oferă titularului drepturilor controlul accesului folosind criptare, dar nu și controlul copierii și redistribuirii. Acest model presupune ca utilizatorii autorizați să aibă echipament special pentru recepționarea și decriptarea materialelor.
- *Model IV*: Acest model permite titularului drepturilor controlul accesului, copierii și redistribuirii, folosind criptografia. Acest model solicită, de asemenea, echipament special pentru accesarea și decriptarea materialelor.
- *Model V*: Acest model permite titularului drepturilor controlul accesului, copierii și redistribuirii prin rețele digitale prin marcarea cu informații de autorizare a folosirii (*watermark*).

Remedii penale și civile se aplică în situații de fabricare, comercializare sau distribuire a echipamentelor de circumvenție (spre exemplu, programe informatice care "sparg" protecția oferită prin criptare)[314]: înlăturarea, evitarea, dezactivarea proceselor, mecanismelor sau sistemelor care împiedică încălcarea drepturilor titularilor[315]. Dreptul de autor trebuie să se adapteze pentru a susține aceste tehnologii noi[316]. Sistemele DRM oferă multe promisiuni, cu toate acestea, există numeroase semne de întrebare sau probleme în ceea ce privește securitatea, interoperabilitatea și integrarea acestora.

Rămân multe aspecte legale nerezolvate (spre exemplu, mecanisme de plată, taxe asociate, protecția consumatorilor, protecția intimității ș.a.)[317]. Limitări în ceea ce privește protecția prin sisteme DRM sunt absolut necesare: folosirea cu justă cauză permite fluxul liber al informațiilor, libertatea de exprimare, comentarea sau critica lucrărilor existente, crearea de lucrări noi și libera competiția.

---

[313] Vezi clasificarea propusă de L. S. Sobel, *DRM as an Enabler of Business Models: ISPs as Digital Retailers*, 2003.

[314] *Nihil tam munitum quod non expugnari pecuna possit.*

[315] Vezi J. E. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 Berkeley Technology Law Journal, 161, 1997.

[316] Vezi M. A. Lange, *Digital Music Distribution Technologies Challenge Copyright Law: A Review of RIAA v. MP3.com and RIAA v. Napster*, Boston B. Journal, Mar.–Apr., 14, 2001.

[317] Vezi R. Ashtar, *Licensing as digital rights management, from the advent of the web to the iPad*, 13 Yale Journal of Law and Technology 141, 2011; C. S. Yoo, *Beyond network neutrality*, Harvard Journal of Law & Technology, 19, 1, 2005; R. M. Frieden, *Universal service: when technologies converge and regulatory models diverge*, Harvard Journal of Law & Technology, 13, 3, 2000.

3.3 Drepturi de proprietate industrială

3.3.1 Protecția semnelor distinctive

Protecţia semnelor distinctive urmăreşte stimularea şi asigurarea unei competii economice corecte şi protejarea consumatorilor, prin posibilitatea de a realiza alegeri informate între bunuri şi servicii. Protecţia acestor semne poate fi pe o durată indefinită, atât timp cât rămân distinctive.

3.3.1.1 Mărci

O "marcă" poate fi un cuvânt, nume, frază[318] sau simbol folosit pentru a identifica un produs sau serviciu[319] (cu alte cuvinte, "semnătura comercială a producătorului") şi are o importantă funcţie de comunicare (publicitate, marketing). Valoarea primară a unei mărci de comerţ moderne constă în reflexul condiţionat dezvoltat în consumatori, în puterea acesteia de a vinde un produs sau serviciu. În unele cazuri, valoarea unei mărci, independent de activele tangibile ale deţinătorului, poate fi estimată la miliarde de dolari (spre exemplu, Coca-Cola).

Mărcile identifică bunuri sau servicii oferite consumatorilor şi sunt considerate o formă de proprietate. Doarece mărcile pot avea o valoare comercială foarte importantă, managementul şi protecţia acestora se bucură de o importanţă aparte[320]. Protecţia mărcilor se bazează pe proceduri de înregistrare[321].

Pentru a facilita protecţia internaţională a mărcilor au fost semnate un număr de acorduri[322]. Tratatul de la Singapore privind dreptul mărcilor[323] (*Singapore Treaty on the Law of Trademarks*) a intrat în vigoare în 16 martie 2009. Acest Tratat actualizează Tratatul dreptului mărcilor (1994) şi permite folosirea avantajelor create de dezvoltările tehnologice din domeniul informaţiei şi

---

318 Spre exemplu, marca Apple "There's an app for that."

319 În 17 septembrie 2014, Apple a aplicat pentru înregistrarea ca marcă de comerţ a Apple "Pay" (*application number 86393745*), în cadrul *International Class 036*, care acoperă servcii financiare, tranzacţii financiare securizate etc.

320 Vezi, spre exemplu, lista de mărci a Apple, Inc., disponibilă la locaţia https://www.apple.com /legal/intellectual-property/trademark/appletmlist.html.

321 Mărcile neînregistrate sunt protejate în anumite jurisdicţii, dar numai o înregistrare legală a acestora poate oferi o protecţia adecvată. Cea mai veche înregistrare a unei mărci în SUA, spre exemplu, datează din anul 1870. În anul 2007, au fost înregistrate 39945 aplicaţii internaţionale pentru mărci de către WIPO, conform sistemului de la Madrid pentru înregistrarea mărcilor, o creştere de 9.5% faţă de anul 2006 (vezi detalii la locaţia http://trademarknews.com/news/record-number-of-international-trademark-filings-in-2007.html).

322 Vezi J. Schmidt-Szalewski, *The international protection of trademarks after the trips agreement*, Duke Journal of Comparative & International Law, 9, 1998; I. Macovei, *Protecţia internaţională a mărcilor*, Revista Română de Dreptul Proprietăţii Intelectuale, V, 3 (16), 2008.

323 Acest Tratat a fost finalizat în martie 2006. România a ratificat Tratatul în 25 martie 2008. SUA au ratificat Tratatul în 1 octombrie 2008.

comunicaţiilor pentru aplicaţii de înregistrare şi procesare a acestora[324]. Conform noilor reglementări, noi tipuri de mărci, cum ar fi mărci holograme, mărci animate, mărci colorate şi mărci care constau din semne non-vizibile, cum ar fi sunete sau gusturi[325], vor putea fi înregistrate[326].

Mărcile de comerţ faimoase oferă, de regulă, garanţia calităţii şi prezintă un interes deosebit pentru cei care încearcă să profite de pe urma investiţiilor făcute de deţinătorul mărcii deoarece aceasta le permite o recunoaştere imediată şi un cost de promovare substanţial redus. Dreptul mărcilor de comerţ protejează împotriva folosirii comerciale a mărcilor cu scopul de a induce în eroare, permiţând producătorilor să creeze o modalitate facilă de identificare a propriilor produse sau servicii şi să reducă costul căutării unui produs pentru consumatori. Firmele au drepturi de proprietate asupra mărcilor de comerţ numai în măsura în care este necesară prevenirea folosirii neautorizate care poate induce în eroare consumatorii.

Protecţia mărcilor de comerţ este "incoerentă"[327], complexă şi neunitară la nivel global[328]. Instrumentele legale internaţionale includ *Convenţia de la Paris* pentru Protecţia Proprietăţii Industriale (1883); *Protocolul Madrid* (*Madrid Protocol Relating to the Madrid Agreement Concerning International Registration of Marks* (1996, ca extensie a *Madrid Agreement* din 1891); *Tratatul Dreptului Mărcilor de Comerţ* (*Trademark Law Treaty*, care prevede standardizarea aspectelor procedurale ale procesului de înregistrare a mărcilor); *Acordul TRIPS* (*Agreement on Trade Related Aspects of Intellectual Property Rights*, 1994)[329], care stabileşte compatibilitatea legală între jurisdicţiile membre prin solicitarea armonizării legilor aplicabile şi conţine prevederi privind mărcile faimoase care suplimentează şi lărgesc domeniul protecţiei solicitat de Convenţia de la Paris [Art. 16 (2) şi (3)]; *Tratatul de la Singapore* (2009), care actualizează Tratatul Dreptului Mărcilor şi permite folosirea avantajelor create de dezvoltările tehnologice din domeniul informaţiei şi comunicaţiilor pentru aplicaţii de înregistrare şi procesare a acestora.

Încălcările privind mărcile sunt similare încălcărilor privind dreptul de autor. Tehnologiile informaţiei moderne şi caracteristicile mediului online creează numeroase oportunităţi de folosire neautorizată a mărcilor de comerţ, printre altele prin intermediul *cybersquatting* (înregistrarea ilegală a unui domeniu cu nume identic sau similar cu o marcă), *typosquatting*, *facesquatting*, *cybergriping*, *meta*

---

324 A se vedea Tratatul la locaţia http://www.wipo.int/treaties/en/ip/singapore.

325 Tratatul de la Singapore nu include reguli standard care să stipuleze modul în care astfel de mărci pot fi incluse în aplicaţia de înregistrare.

326 A se vedea, pentru detalii, C. R. Romiţan, *Protecţia penală a proprietăţii intelectuale*, Ed. C.H. Beck, Bucureşti, p. 301-304, 2006; L. Mocanu, *Tipuri de mărci care pot fi înregistrate. Abordare comunitară şi naţională*, Revista Română de Dreptul Proprietăţii Intelectuale, V, 3 (16), 2008; E. E. Marin, *De ce nu se poate înregistra un semn descriptiv ca marcă*, Revista Română de Dreptul Proprietăţii Intelectuale, V, 2 (15), 2008. Vezi şi *Madrid System International Registry*.

327 Vezi, spre exemplu, Deven R. Desai, *A Brand Theory of Trademark Law*, 2010.

328 Vezi, spre exemplu, Kenneth L. Port, *Protection of Famous Trademarks in Japan and the United States*, 15 Wisconsin International Law Journal 259, 1997.

329 Vezi Katherine Beckman şi Christa Pletcher, *Expanding Global Trademark Regulation*, Wake Forest Intellectual Property Law Journal, Vol. 10, No. 2, 2009-2010.

tag-urilor sau prin publicitatea contextuală. Cel mai serioase încălcări în acest domeniu sunt reprezentate de folosirea de mărci în activităţi criminale cu scopul de a induce în eroare persoanele vizate şi de folosirea acestora în numele de domeniu Internet (*cyber-squatting*). Numele de domeniu facilitează găsirea locaţiilor pe Internet şi permit firmelor să promoveze nume care să le identifice, să le distingă de alte firme şi, implicit, să atragă sau să reţină clienţi.

Originile legislaţiei SUA în domeniul mărcilor pot fi regăsite în delictul de înşelăciune şi în dreptul competiţiei neloiale. *Trademark Act* a fost creat iniţial în 1870, invalidat de Curtea Supremă în 1879; au urmat *Trademark Act* din 1881, cel din 1905, amendat în 1920 şi înlocuit de *Lahnam Trademark Act* din 1946 (amendat în 1962). În 1995 a fost adoptat *Federal Trademark Dilution Act* (FTDA), care incorporează o clauză federală de diluare în Lanham Act ("diluarea" este definită ca fiind reducerea capacităţii unei mărci faimoase de a identifica şi distinge bunuri sau servicii, indiferent de prezenţa sau absenţa competiţiei între deţinătorul mărcii faimoase şi celelalte părţi sau de probabilitatea unei confuzii, greşeli sau înşelăciuni), urmat în iunie 2006 de *Trademark Dilution Revision Act* (TDRA, 15 U.S.C. § 1125 (2006)), care vizează o protecţie mărită pentru mărcile de comerţ faimoase[330].

Legislaţia Uniunii Europene în domeniul mărcilor de comerţ include Directiva privind mărcile (*Trade Marks Directive*, 2008/95/EC, OJ L 299, 8.11.2008), care defineşte "marca de comerţ" (Art. 2) şi vizează înlăturarea disparităţilor din domeniul dreptului mărcilor, care pot împiedica libera circulaţie a bunurilor, libertatea de a furniza servicii şi poate duce la distorsionarea competiţiei economice; *Trademark Regulation*, adoptată în 1993 (în vigoare din 1994); *Council Regulation (EC) No. 207/2009 on the Community Trade Mark* (care înlocuieşte *Trademark Directive* din 1989): conform acesteia, o marcă are un caracter unitar la nivel comunitar (vezi Art. 1) şi se înfiinţează *Office for Harmonisation in the Internal Market* (*Trade Marks and Designs*) care permite înregistrarea de mărci la nivel european (vezi Art. 2).

Aspecte privind folosirea mărcilor de comerţ în pagini web[331]

Unele practici legate de atragerea clienţilor către locaţii web ating aspecte privind mărcile de comerţ deoarece crează confuzie, diluarea valorii mărcii de comerţ şi alte forme de exploatare abuzivă. Practicile abuzive de acest tip includ folosirea mărcilor de comerţ ca *metatag*-uri, vânzarea de cuvinte cheie (*keywords*) care includ mărci de comerţ, reclame de tip *pop-up* şi *linking* sunt descrise pe scurt în cele ce urmează.

---

330 Pentru discuţii academic pe tema diluării unei mărci, a se vedea Barton Beebe, *The Continuing Debacle of U.S. Antidilution Law: Evidence from the First Year of Trademark Dilution Revision Act Case Law*, 24 Santa Clara Computer & High Tech Law Journal, 449, 2008; Justin J. Gunnell, *Goldilocks and the Three Federal Dilution Standards: An Empirical Review*, 17 Texas Intellectual Property Law Journal 101, 2008.

331 Vezi o prezentare detaliată a aspectelor din această secţiune în World Intellectual Property Organization, *Intellectual property on the Internet: A survey of issues*, 2002.

Folosirea mărcilor de comerț ca metatag-uri

Un "metatag" (numit și "meta data") este un cuvânt sau frază cheie în codul HTML (limbajul *hypertext markup*) folosit pentru a facilita motoarelor de căutare identificarea și categorizarea conținutului unei pagini web. Metatag-urile sunt vizibile pentru utilizatori doar prin accesarea codului sursă al paginii web.

În mai multe țări, au apărut dispute privind utilizarea neautorizată a mărcilor de comerț ca metatag-uri, complexitatea problemei este ilustrată de cazurile Playboy Magazine. În *Playboy Enterprises Inc. v. Calvin Designer Label*[332] curtea a decis să împiedice folosirea mărcilor "Playboy" și "Playmate" ca metatag-uri în cadrul locațiilor web sau în numele de domenii. În cazul *Playboy Enterprises Inc. v. Welles*[333], s-a considerat că folosirea metatag-ului Playmate de către o fostă "Playmate of the year" pentru a permite consumatorilor localizarea paginii web este folosire îndreptățită (*fair use*). O decizie similară a fost în cazul *Playboy Enterprises v. Netscape Communications*[334], curtea considerând că folosirea mărcii de comerț ca metatag de către motorul de căutare al acuzatului este folosire îndreptățită.

Vânzarea de cuvinte cheie

Acest tip de practică este considerată că îndepărtează potențielii clienți de la locațiile deținătorilor mărcilor de comerț. În cazul *Playboy Enterprises Inc. v. Netscape Communications Corporation*, curtea a considerat că "Playboy" și "Playmate" trebuie considerate *cuvinte generice*, nu mărci de comerț.

Reclame de tip *Pop-Up*

Reclamele de tip pop-up sunt ferestre care nu sunt lansate/inițiate de către utilizatori. Prin efectuarea unui click asupra unui element din fereastra pop-up, utilizatorul va fi redirectat către locația web a beneficiarului. Asemenea practici pot reprezenta încălcări ale mărcilor[335].

Linking

Tehnologiile de acest tip permit utilizatorilor accesarea de informații stocate în fișiere stocate pe același calculator sau pe alte calculatoare, dar ridică și problema încălcării mărcilor de comerț dacă sugerează, implicit sau explicit, o asociere între locațiile implicate, inducând utilizatorilor idea că ar exista o asociere între părțile implicate. Incorporarea de materiale sau *linking*[336] la o locație care încalcă drepturi de proprietate intelectuală ridică, de asemenea, probleme juridice dificile[337].

---

332 Playboy Enterprises, Inc. v. Calvin Designer Label, 985 F. Supp. 1220 (N.D. Cal. 1997).
333 Playboy Enterprises, Inc. v. Welles, 279 F.3d 796 (9th Cir. 2002).
334 Playboy Enterprises v. Netscape Communications, 354 F.3d 1020 (9th Cir. 2004).
335 Vezi Janet Rubin, *Pop-Up Ads and Trademark I14nfringement: WhenU.com Litigation*, Cardozo Arts & Entertainment, Vol. 24, 323-347, 2006.
336 Flava Works, Inc. v. Gunter, 689 F.3d 754 (2012).
337 Vezi Eldar Haber, *Copyrighted crimes: The copyrightability of illegal works*, 16 Yale Journal of Law & Technology, 454-501, 2014.

Cazuri

Rescuecom Corp. v. Google Inc.[338]

Corporaţia Rescuecom, care furnizează servicii informatice, deţine marca RESCUECOM. În acest caz, au fost aduse în discuţie programele *Google AdWords* (acesta manipulează rezultatele unei căutări Google pentru a ierarhiza artificial o pagină web înaintea altora; firmele care doresc publicitate putând achiziţiona reclame bazate pe numele unor competitori) şi *Google Keyword Suggestion Tool* (care recomandă potenţiale cuvinte cheie pentru reclame care să fie folosite în programul *AdWords*).

Aspectul esenţial al procesului a constat în a stabili dacă folosirea de către Google a mărcii RESCUECOM în ambele programe consituie folosire comercială (*use in commerce*) conform § 1127 al Lanham Act (Rescuecom a susţinut că este încălcare dacă Google permite competitorilor Rescuecom să achiziţioneze reclame care sunt afişate când un utilizator efectuează o căutare după cuvântul-cheie "rescuecom"). Conform Rescuecom, marca sa este folosită comercial deoarece Google beneficiază de pe urma sa, crează confuzie în rândul utilizatorilor Internet şi împiedică utilizatorii să ajungă la propia pagină web (care primeşte, în medie, 17.000-30.000 vizitatori în fiecare lună).

În 2006, United States District Court for the Northern District of New York a acceptat argumentul Google conform căruia folosirea mărcii RESCUECOM a fost *internă* şi nu constituie o încălcare prin folosire comercială (folosirea "internă" a unei mărci nu este suficientă, în mod automat, mărcile, în asemenea cazuri, sunt "citite" de calculatoare, nu de către consumatori), Google neplasând marca RESCUECOM pe bunuri, containere sau reclame.

La apel (2009), Second Circuit a considerat că Google a folosit în comerţ marca RESCUECOM, iar acţiunile sale pot fi considerate acţionabile conform secţiunilor 32 şi 43 ale Lanham Act (15 U.S.C. sections 1114 şi 1125) şi a trimis cazul pentru reexaminare (*remanded*)[339]. În martie 2010, Rescuecom a renunţat la acţiunea legală împotriva Google şi a anunţat că Google a încetat folosirea mărcilor în textul reclamelor sponsorizate[340].

---

338 Rescuecom Corp. v. Google Inc., 562 F.3d 123, 129–30 (2d Cir. 2009).

339 Acest caz prezintă un interes deosebit şi este amplu discutat în literatura de specialitate - vezi discuţii extinse în Ashley Tan, *Google AdWords: Trademark Infringer or Trade Liberalizer?*, Michigan Telecommunications and Technology Law Review, Vol. 16, 2010; Tyson Smith, *Googling a Trademark: A Comparative Look at Keyword Use in Internet Advertising*, Texas International Law Journal, Vol. 46, 2010; Jessica A.E. McKinney, *Rescuecom Corp. v. Google Inc.: A Conscious Analytical Shift*, 95 Iowa Law Review, 2009. A se vedea, in acest context, şi Jonathan Cornthwaite, *To Key or Not to Key? The Judgment of the European Court of Justice in the Google France AdWords Cases*, European Intellectual Property Review, 352, 2010; *European Court of Justice holds that search engines do not infringe trademarks* - Joined Cases C-236/08, C-237/08 & C-238/08, Google France SARL v. Louis Vuitton Malletier SA, 2010 ECJ EUR-Lex LEXIS 119 (Mar. 23, 2010), Harvard Law Review, Vol. 124, 2010.

340 Vezi declaraţia firmei, la locaţia http://www.rescuecom.com/a-case-of-david-versus-googleiath.html.

Sellify Inc. c. Amazon.com, Inc.[341]

Prin intermediul *Associates Program*, Amazon.com permite unui număr de peste trei milioane de persoane fizice și juridice să aibă link-uri la propriul site. Dacă un client ajunge la site-ul Amazon prin intermediul unui click pe un link al unui asociat, acesta din urmă primește un mic procent din achizițiile făcute pe Amazon.com într-un interval de 24 de ore. Ca parte a acestui program, Amazon permite folosirea propriului logo în reclamele online (nemonitorizând aceste reclame, asociații fiind responsabili, conform *Associates Program Operating Agreement*, de conținutul propriilor reclame). În situațiile în care un asociat încalcă prevederile din *Agreement*, acesta poate fi exclus din program.

Doi asociați sunt implicați în acest caz: *OneQuality*, deținut și operat de Sellify și *Cutting Edge Designs*. În martie 2009, Cutting Edge a achiziționat cuvântul-cheie "onequality.com" de la Google, Inc. Ca urmare, de fiecare dată când un utilizator Google efectuează o căutare <onequality.com>, rezultatul căutării va afișa o reclamă "Don't Buy from Scammers" și "Beware the SCAM Artists", cu link la site-ul <amazon.com>.

După ce a văzut aceste reclame, deținătorul Sellify și OneQuality, a contactat Amazon, care l-a informat că nu poate face nimic în această privință. Fiind amenințată cu o acțiune în instanță, Amazon a trimis o scrisoare către Cutting Edge, anunțând că va închide contul lor dacă nu încetează reclamele în cauză (acest lucru s-a realizat ulterior). În acțiunea intentată, Sellify a acuzat încălcări ale Lanham Act și competiție neloială. Amazon a solicitat *summary judgment*[342].

În cauză s-a decis că un furnizor de servicii online nu poate fi făcut responsabil direct conform Lanham Act pentru acte ale unei terțe părți. Adițional, un furnizor de servicii online nu poate fi făcut răspunzător pentru contribuție la încălcarea unei mărci deoarece nu avea suficientă cunoștință despre încălcare și nici nu a mai furnizat serviciul după ce a fost notificat despre încălcarea în cauză.

Nine West Dev. Corp. v. Does 1-10, 07-cv-7533-DLC

Nine West, o firmă importantă în domeniul articolelor de îmbrăcăminte, încălțăminte și accesorii pentru femei, ale cărei produse sunt vândute în multe țări, deține marca de comerț NINE WEST. Acuzații din acest caz, cu identități necunoscute la momentul depunerii plângerii, au creat un cont "NineWest Shoes" pe Facebook și au folosit, reprodus și/sau copiat fără autorizare sau licență marca NINE WEST în vederea realizării unei scheme frauduloase care urmărea crearea impresiei că firma realizează audiții pentru tinere modele feminine. Cel puțin 400 de persoane au accesat respectivul cont Facebook și au trimis informații personale și fotografii.

În cadrul acțiunii civile, firma Nine West a adus următoarele acuzații: încălcare deliberată și cu rea credință a mărcii NINE WEST (conform Section 32

[341] Sellify Inc. v. Amazon.com, Inc., No. 09 Civ. 10268 (JSR). (S.D.N.Y. Nov 04, 2010).

[342] *Summary judgment* este o determinare făcută de o instanță fără un proces deplin, pe baza meritelor întregului caz sau a problemei specifice aflată în discuție; este folosită când nu se dispută fapte sau evidențe într-un caz, iar una din părți este îndreptățită la o decizie.

BCU IAȘI CENTRAL UNIVERSITY LIBRARY

al Lanham Act), desemnare falsă a originii şi descriere şi reprezentare falsă (conform Section 43 (a) a Lanham Act), diluarea mărcii (*tarnishment*) (conform Section 43 (c) a Lanham Act), precum şi folosirea de practici comerciale care induc în eroare şi crearea de publicitate falsă.

Firma Nine West a informat Facebook despre anunţul fraudulos şi a solicitat ştergerea permanentă a Nine West Audition Group, revocarea "NineWest Shoes" şi notificarea membrilor grupului despre folosirea frauduloasă (lucruri realizate după două zile). La scurt timp după accea, a apărut un nou grup pe Facebook, numit "Nine West – Model Auditions". Nine West a contactat Facebook în vederea revocării noului grup.

În cadrul plângerii depuse de Nine West în 2007, se solicita interzicerea folosirii de către acuzaţi de conturi Facebook care conţin marca NINE WEST sau orice variaţie sau derivaţia a acesteia care pot cauza confuzie pentru utilizatori şi acordarea de daune compensatorii şi punitive.

Visa Inter. Ser. Ass'n v. JSL Corp.[343]

Joseph Orr deţine *eVisa*, un serviciu de educaţie multilinguală şi informaţii de afaceri care există şi operează exclusive pe Internet, la adresa *www.evisa.com*. Orr explică numele *eVisa* ca provenind de la un serviciu de învăţare a limbii engleze numit "Eikaiwa Visa" (în limba japoneză "Eikaiwa" înseamnă conversaţie în engleză, "e" fiind prescurtarea pentru acest cuvânt) pe care îl deţinea când trăia în Japonia. Folosirea cuvântului "visa" în *eVisa* şi Eikaiwa Visa intenţionează să sugereze "capacitatea de a călătorii, lingvistic şi fizic, prin lumea de limbă engleză".

Visa International Service Association a acţionat în instanţă JSL Corporation, prin intermediul căreia Orr operează *eVisa*, susţinând că *eVisa* diluează marca de comerţ VISA, marcă faimoasă în întreaga lume, aducând şi studii de piaţă şi depoziţii ale experţilor care susţin acest lucru. Instanţa districtuală a acordat *summary judgment* pentru Visa, JSL făcând apel.

Mărcile din acest caz sunt practic identice, singura diferenţă fiind prefixul "e", folosit în mod curent pentru referire la versiuni electronice sau online ale unei mărci. JSL a susţinut că marca *eVisa* nu poate cauza diluare deoarece, atunci când o marcă este şi un cuvânt cu definiţie în dicţionar, este dificil să se demonstreze că marca este suficient de distinctivă pentru a se bucura de protecţie împotriva diluării (chiar dacă JSL nu foloseşte cuvântul "visa" pentru definiţia sa literală). Folosirea mărcii *eVisa* pentru servicii de învăţare a limbii engleze nu încalcă marca VISA pentru servicii de carduri de credit; mărcile sunt similare, dar serviciile sunt atât de diferite încât nu se pune problem confuziei între acestea, situaţie în care demonstrarea diluării mărcii devine aproape imposibilă.

În SUA, mărcile faimoase au o protecţie sporită împotriva diluării, fiind necesară doar "posibilitatea" ca acestea să fie diluate, pentru o pronunţare favorabilă. O marcă asociată cu un produs poate fi asociată cu un alt produs, ceea ce micşorează capacitatea mărcii de a evoca primul produs în mintea

[343] Visa Inter. Ser. Ass'n v. JSL Corp., 610 F.3d 1088 (9th Cir. 2010).

consumatorilor (*dilution by blurring*). Prin urmare, în acest caz s-a decis că marca *eVisa* diluează marca VISA conform 15 U.S.C. § 1125(c)(2)(B) (2006) (marca VISA poate fi diluată de un alt utilizator care nu folosește cuvântul conform înțelesului larg). Instanța a menținut decizia de *summary judgment*.

3.3.1.2 Indicații geografice

Semnele distinctive identifică produse și servicii în relație cu calitățile, sursa sau originea lor sau alte caracteristici care permit consumatorilor să le distingă de alte produse sau servicii. Protejarea acestor semne împotriva însușirii nejustificate sau a folosirii neautorizate asigură competiția loială, permite producătorilor folosirea lor ca instrumente de marketing puternice și permite consumatorilor să selecteze în mod informat produse[344]. Semnele distinctive includ nume de comerț, mărci de comerț și *indicații geografice*.

Indicațiile geografice sunt nume sau etichete folosite pe produse cu o anumită origine geografică și care au anumite calități sau se bucură de o anumită reputație, atribuită esențial respectivei proveniențe. Indicațiile geografice sunt folosite pentru a desemna calitatea unui produs, pentru a evidenția identitatea acestuia și a prezerva tradiții culturale[345]. De asemenea, specificațiile unui produs în contextul indicațiilor geografice contribuie semnificativ la consistența calității produsului[346].

Calitățile unui produs sunt derivate din factori geografici, cum ar fi clima sau altitudinea, proveniența materiilor prime, sau a factorilor umani implicați, cum ar fi modalitățile de preparare sau procesare. Exemple de astfel de produse ar fi, la nivel internațional, *Tequila* (Mexic), *Nakhornchasi Pomelo* (Tailanda), *Darjeeling* (India), *Kobe* (Japonia), *Cacao Arriba* (Ecuador) sau *Cacao de Chuao* (Venezuela); la nivelul Uniunii Europene printre cele mai cunoscute se numără *Champagne*, *Sherry*, *Porto*, *Chianti*, *Samos*, *Moselle Luxembourgeoise* (vinuri); *Cognac*, *Brandy de Jerez*, *Grappa di Barolo*, *Genièvre Flandres Artois*, *Scotch Whisky*, *Tsikoudia* (băuturi spirtoase); *Roquefort*, *Prosciutto di Parma*, *Gorgonzola*, *Aziete de Moura*, *Olive de Kalamata*, *Coquille Saint-Jacques des Côtes-d'Amour*, *Jamón de Huelva* etc. (alte produse).

Termenul generic 'indicații geografice' include un număr de concepte, incluzând indicații de sursă și denumiri de origine. Conform *The Agreement on Trade-related Aspects of Intellectual Property Rights* (*The TRIPS Agreement*) 'indicațiile geografice' identifică un bun ca fiind original dintr-un anumit teritoriu, regiune sau localitate, unde o anumită calitate, reputație sau alte caracteristici ale bunului pot fi atribuite esențial originii sale geografice (Art. 22(1)). Definiții similare pot fi găsite în *North American Free Trade Agreement* (Art. 1721), și în

---

[344] Vezi M. J. Oliva, *Geographical Indications: Distinguishing the Uniqueness of BioTrade Products*, 2007; World Bank, *Global Economic Prospects and the Developing Countries 2002: Making Trade Work for the World's Poor*, World Bank, Washington DC, 143-144, 2001.

[345] Vezi la http://www.geographicindications.com.

[346] Vezi M. J. Oliva, op. cit.

BCU IASI CENTRAL UNIVERSITY LIBRARY

European Commission Regulation No. 2081/92 din 14 iulie 1992 (OJ L 208, 24.7.1992, p. 1), privind protecția indicațiilor geografice și a desemnărilor de origine pentru produsele agricole (Art. 2)[347].

În România, Legea nr. 84 din 15 aprilie 1998 definește 'indicația geografică' ca fiind "denumirea servind la identificarea unui produs originar dintr-o țară, regiune sau localitate a unui stat, în cazurile în care o calitate, o reputație sau alte caracteristici determinate pot fi în mod esențial atribuite acestei origini geografice" (Art. 3f).

Indicațiile geografice prezintă o serie de similarități cu mărcile de comerț. Astfel, ambele indică originea unor bunuri, garantează calitatea unui bun și pot consitui brand-uri comerciale valoroase, dar și diferențe importante (indicațiile geografice sunt nume geografice, considerate descriptive, deci neprotejabile, în doctrina mărcilor de comerț[348]).

În ciuda similarităților funcționale, indicațiile geografice diferă de mărcile de comerț în următoarele privințe[349]:

- Spre deosebire de o marcă de comerț, care are de regulă un singur deținător înregistrat, în protecția indicațiilor geografice există un interes colectiv;
- Pentru înregistrarea unei mărci de comerț, aceasta trebuie să fie distinctă, în timp ce indicațiile geografice sunt folosite de toți producătorii dintr-o zonă;
- Indicațiile geografice generează interese specifice, dincolo de tradiționala protecție a consumatorilor și producătorilor, specifică dreptului mărcilor de comerț;
- Mărcile de comerț pot fi licențiate unor terțe părți, spre deosebire de indicațiile geografice[350].

În anumite circumstanțe, indicațiile geografice pot fi înregistrate ca mărci de comerț: când aceste indicații nu au în principal o semnificație geografică pentru publicul relevant sau când consumatorii nu vor putea considera că produsele au fost produse în acel loc (spre exemplu, Amazon.com™ este înregistrată pentru

---

347 Vezi și WIPO, *What is geographical indications?* Available at http://www.wipo.int/about-ip/en/index.html; accessed on February 4, 2002.

348 De remarcat că, în SUA, se consideră că indicațiile geografice servesc aceeași funcție ca mărcile de comerț, deoarece, precum mărcile de comerț, sunt identificatori de sursă, garanție a calității și interese de afaceri importante. Unele patente acordate în SUA de United States Patent and Trademark Office (USPTO) se bazează pe indicații geografice din alte țări (spre exemplu, *orez Basmati* din India, *orez Jasmine* din Tailanda sau *Ayahuasca*, băutură ceremonială preparată, de multe generații, de șamanii triburilor din bazinul râului Amazon prin procesarea cojilor de Banisteriopsis caapi), ceea ce a declanșat numeroase proteste și chiar procese legale.

349 Vezi D. Gangjee, *Protecting Geographical Indications as Collective Trademarks: The Prospects and Pitfalls*, IIP Bulletin, p. 112, 2006.

350 Vezi S. Stern, *Worldwide Symposium on Geographical Indications* organized by the World Intellectual Property Organization (WIPO) and the United States Patent and Trademark Office (USPTO), San Francisco, California, 2003.

BCU CLUJ / CENTRAL UNIVERSITY LIBRARY

cărți sau alte produse, nici un consumator rezonabil neputând considera că firma este localizată în zona Amazon[351]).

Protecția indicațiilor geografice

Problema protecției indicațiilor geografice a fost și este subiect intens de dezbatere la nivel mondial[352]. Există un conflict esențial între protecția cele două: susținătorii indicațiilor geografice văd aceste denumiri ca absolute, adică, odată create acestea trebuie să asigure exclusivitate chiar dacă aceasta implică eliminarea unor drepturi în mărci de comerț valide, pre-existente, în timp ce susținătorii mărcilor de comerț consideră că principiul "primului venit" trebuie folosit în cazul conflictului între indicații geografice și mărci de comerț[353].

Indicațiile geografice sunt protejate în acord cu legi naționale, sub un număr larg de concepte, cum ar fi protecția consumatorilor, competiția neloială, protecția denumirilor de origine și a mărcilor de certificare. La nivel internațional, o serie de tratate administrate de Organizația Mondială a Proprietății Intelectuale (OMPI) oferă o anumită protecție indicațiilor geografice:

- *The Paris Convention for the Protection of Industrial Property* din 1883, deși nu definește 'indicațiile geografice' ci folosește termeni diferiți ("indicații de sursă" și "denumire de origine");
- *The Madrid Agreement on Indications of Source* din 1891;
- *The Lisbon Agreement for the Protection of Appellations of Origin* din 1958, care definește "denumirile de origine" ca fiind "nume geografice de țară, regiune sau localitate, care servesc la desemnarea unui produs cu originea din acel loc, calitățile și caracteristicile acestuia datorându-se exclusiv sau esențial mediului geografic, incluzând factori naturali sau umani", iar "țara de origine" este definită ca fiind "țara al cărei nume sau țara în care este situată regiunea sau localitatea al cărei nume constituie denumirea de origine care a dat produsului reputația de care se bucură".

---

[351] Vezi în D. Gangjee, op. cit.

[352] Vezi, spre exemplu, D. Troskie, *Geographical indications at the national level a variety of approaches and institutional aspects*, International Symposium on Geographical Indications jointly organized by the World Intellectual Property Organization (WIPO) and the State Administration for Industry and Commerce (SAIC) of the People's Republic of China Beijing, 2007; G. E. Evans și M. Blakeney, *The Protection of Geographical Indications After Doha: Quo Vadis?*, Journal of International Economic Law, Vol. 9 No. 3, 2006; M. Maher, *On vino veritas? Clarifying the use of geographic references on American wine labels*, California Law Review, Vol. 89, Iss. 6, 1881-1925, 2001; E. K. Meltzer, *Pass the Parmesan? What You Need to Know About Geographical Indications and Trademarks*, Virginia Lawyers Weekly, June/July, 2002; European Communities Trade Mark Association, *Report on the Worldwide Symposium on Geographical Indications*, Parma, Italy, 2005; A. Nyaga, *The Geographical Indication Protection Africa Perspective*, WTO Round Table on Geographic Indications, 2004; WIPO, *Symposium on the international protection of geographical indications*, 2000; WIPO, *Possible solutions for conflicts between trademarks and geographical indications and for conflicts between homonymous geographical indications*, 2000.

[353] A se vedea în acest context cazul Torres, în care marca de comerț TORRES a fost înregistrată și folosită pentru o anumită perioadă de timp, ea venind în conflict cu "Torres Vedras", declarată indicație geografică de guvernul Portugaliei.

- The Agreement on Trade-related Aspects of Intellectual Property Rights (*The TRIPS Agreement*), care stabileşte regimul legal pentru indicaţiile geografice care există în contextul Organizaţiei Mondiale a Comerţului [*World Trade Organization* (WTO)] şi care este folosit în cazul disputelor din cadrul acestui sistem. Astfel, Articolul 22 al *TRIPS Agreement* defineşte un nivel general de protecţie[354], în timp ce Articolul 23 stabileşte un nivel de protecţia a indicaţiilor geografice pentru vinuri şi băuturi spirtoase mai elaborat. Articolul 24 stabileşte un număr de excepţii şi prevederi legate de Articolele 22 şi 23. Conform Articolului 24.9, ţările care solicită protecţia unor denumiri geografice trebuie să le protejeze întâi la ele acasă.

Adiţional, o serie de organizaţii, cum ar fi ORIGIN (*Organisation for an International Geographical Indications Network*), AIPPI (*International Association for the Protection of Intellectual Property*), INTA (*International Trademarks Association*) sau OIV (*International Office of Wine and Vine*) au analizat sau discutat protecţia acordată indicaţiilor geografice. La nivel european, legislaţia[355] cuprinde prevederi pentru înregistrarea, certificarea şi protecţia indicaţiilor geografice, clasificate ca fiind:

- Indicaţii de origine protejate (*Protected Designations of Origin* - PDOs): desemnarea PDO semnifică faptul că produsele sunt "procesate, produse şi preparate într-o arie geografică folosind *know-how* recunoscut";
- Indicaţii geografice protejate (*Protected Geographical Indications* - PGIs): desemnările PGI înseamnă că "legăturile geografice trebuie să apară în cel puţin un stadiu al producţiei, procesării sau preparării";
- Specialităţi tradiţionale garantate (*Traditional Specialty Guaranteed* - TSG): desemnările TSG "nu se referă la originea unui produs ci subliniază un caracter tradiţional, în compoziţie sau în mijloacele de producţie".

În 1992, Uniunea Europeană (UE) a adoptat *EC Regulation No 2081/92 on the Protection of Geographical Indications and Designations of Origin for Agricultural Products and Foodstuffs*. În 19 Aprilie 2005, o comisie a Organizaţiei Mondiale a Comerţului (WTO) a decis în favoarea SUA că reglementările europene (2081/92) nu sunt consistente cu obligaţiile europene conform TRIPS Agreement şi GATT 1994 şi că Uniunea Europeană nu poate refuza protecţia indicaţiilor geografice produselor din terţe ţări ale căror sisteme nu sunt

---

354 În acest articol, se solicită membrilor asigurarea instrumentele legale pentru a preveni:
(a) folosirea oricăror mijloace în desemnarea sau prezentarea unui bun care indică sau sugerează că bunul în cauză provine dintr-o arie geografică alta decât locul de origine într-o manieră care induce în eroare publicul cu privire la originea geografică a produsului;
(b) orice folosire care constituie un act de competiţie neloială în înţelesul Art. 10bis al Convenţiei de la Paris (1967).

355 Vezi *Geographical indications and traditional specialities*, http://ec.europa.eu/agriculture/quality/schemes/index_en.htm.

echivalente[356]. Subsecvent, UE a implementat EC Regulation 510/2006[357], în efect din 31 Martie 2006, care defineşte mai clar sistemul UE pentru recunoaşterea şi înregistrarea indicaţiilor geografice din terţe ţări, permite indivizilor şi grupurilor să aplice pentru înregistrarea indicaţiilor geografice din terţe ţări în UE fără participarea guvernului terţei ţări şi permite o protecţie sporită mărcilor de comerţ preexistente. Adiţional, UE a negociat tratate specifice privind protecţia indicaţiilor geografice privind vinurile şi băuturile spirtoase cu unele ţări (Africa de Sud, Chile, Mexic, SUA ş.a).

În România, indicaţiile geografice ale produselor sunt protejate prin înregistrarea acestora la Oficiul de Stat pentru Invenţii şi Mărci, conform Legii nr. 84/1998 şi a convenţiilor internaţionale la care România este parte. Indicaţiile geografice pot fi folosite numai de persoanele care produc sau comercializează produsele pentru care aceste indicaţii au fost înregistrate (conform Art. 67)[358].

Lista indicaţiilor geografice a căror protecţie este recunoscută în România, pe baza convenţiilor prevăzute de lege, este înscrisă la Oficiul de Stat pentru Invenţii şi Mărci în Registrul Naţional al Indicaţiilor Geografice şi publicată în Buletinul Oficial de Proprietate Industrială. Conform Art. 70, sunt excluse de la înregistrare indicaţiile geografice care:

- Nu sunt conforme dispoziţiilor art. 3 lit. f);
- Sunt denumiri generice ale produselor;
- Sunt susceptibile de a induce publicul în eroare asupra naturii, originii, modului de obţinere şi calităţii produselor;
- Sunt contrare bunelor moravuri sau ordinii publice.

---

356 Vezi *Summary of the Report of the Panel* (WT/DS174/R) din 15 Martie 2005 privind *Complaint by the United States against the European Communities on the Protection of Trademarks and Geographical Indications for Agricultural Products and Foodstuffs*. A se vedea şi *Complaint* WT/DS290/R.

357 Vezi la http://eur-lex.europa.eu.

358 Un caz interesant din practica Î.C.C.J., Secţia civilă şi de proprietate intelectuală, decizia nr. 1993 din 15 martie 2005 a implicat reclamantele S.C. Bachus S.A. şi Asociaţia Tezaurul de la Pietroasa, care au chemat în judecată S.C. Vincon Vrancea S.A. (titulara mărcilor "Proles Pontica" şi "Vinuri de aur tradiţionale") şi au solicitat ca aceasta să fie obligată să înceteze folosirea în activitatea sa de comunicat a mărcii "Pietroasa" şi a menţiunii "Pietroasele" care, datorită identităţii/similarităţii cu marca „Pietroasa" şi indicaţia geografică "Dealu Mare – Pietroasa" crează confuzie în rândul consumatorilor şi să fie obligată să plătească penalităţi. Instanţele de fond şi de apel au reţinut S.C. Vincon S.A. Focşani a indicat corect originea geografică a vinului comercializat (vin provenit de la Staţiunea de Cercetare şi Dezvoltare Vitivinicolă Pietroasa S.A.) prin inserarea pe etichetele folosite a provenienţei geografice a vinului, Podgoria Pietroasele.

Într-adevăr, prin art. 36, art. 67 şi art. 75 din Legea nr. 84/1998, a fost reglementat dreptul exclusiv al titularului de folosire a mărcii sau indicaţiei geografice înregistrate. Art. 38 din Legea nr. 84/1998 prevede, însă, în mod expres, că titularul mărcii nu poate cere să se interzică unui terţ să folosească, în cadrul activităţilor sale comerciale, indicaţii care se referă la calitatea, originea geografică sau orice alte caracteristici ale produsului acestuia. Prevederile Legii nr. 84/1998 trebuie interpretate şi în raport cu dispoziţiile Legii nr. 244/2002 a viei şi vinului, art. 18, lit. b prevăzând obligativitatea de a indica provenienţa geografică, în scopul de a garanta pentru consumator respectarea condiţiilor de calitate şi a caracteristicilor specifice produsului din zona la care se refera indicaţia geografică. Faţă de considerentele menţionate, s-a respins recursul ca nefondat.

Conform Art. 74, durata de protecție a indicațiilor geografice curge de la data depunerii cererii la Oficiul de Stat pentru Invenții și Mărci și este nelimitată. Dreptul de utilizare a indicației geografice se acordă solicitantului pe o perioadă de 10 ani, cu posibilitatea de reînnoire nelimitată, dacă se mențin condițiile în care acest drept a fost dobândit[359].

3.3.2 Stimularea inovației și crearea de tehnologii

3.3.2.1 Brevet de invenție

Un "brevet de invenție" (*patent*) este un document acordat de un oficiu guvernamental, care descrie o invenție (adică, un metodă sau un proces care reprezintă o soluție la o problemă specifică în domeniul tehnologiei) și care crează o situație legală în care invenția brevetată poate fi exploatată (fabricată, folosită, vândută sau importată) doar cu autorizarea deținătorului brevetului de invenție. Protecția conferită de un brevet de invenție reprezintă o modalitate de promovare a inovației și este limitată în timp, de regulă pentru 20 de ani. Sofisticare produselor și competitivitatea foarte ridicată din domeniul tehnologiilor informației și comunicației a generat un număr impresionant de brevete de invenție, de cereri de reexaminare a acestora și de dispute legale. Aflate la confluența dreptului cu tehnologiile avansate, brevetele de invenție prezintă numeroase aspecte controversate, dezbătute intens în literatura de specialitate din ultimii ani[360].

Disputele legale implicând brevete de invenție sunt complexe[361] și, cel mai adesea, pretențioase din punct de vedere tehnic[362]. Domeniu este controversat și pentru că supraprotecția, în loc să stimuleze inovația, împiedică accesul public la

---

[359] Pentru a discuție detaliată a protecției indicațiilor geografice în România, a se vedea M. Păstoreanu, *Protecția juridică a mărcilor și indicațiilor geografice*, Revista Română de Dreptul Proprietății Intelectuale, Anul IV, Nr. 1 (10), 105-113, 2007; A. L. Arjoca, *Apărarea drepturilor asupra mărcilor și indicațiilor geografice*, Revista Română de Dreptul Proprietății Intelectuale, Anul III, Nr. 3 (8), 94-110, 2006.

[360] Vezi Michael Meehan, *Increasing Certainty and Harnessing Private Information in the U.S. Patent System: A Proposal for Reform*, Stanford Technology Law Review 1, 2010; Robert R. Willis, *International Patent Law: Should United States and Foreign Patent Laws Be Uniform? An Analysis of the Benefits, Problems, and Barriers*, North Carolina Journal Of Law & Technology, Vol. 10, Iss. 2, Spring, 2009; Kendra Robins, *Extraterritorial Patent Enforcement and Multinational Patent Litigation: Proposed Guidelines for U.S. Courts*, Virginia Law Review, Vol. 93, 2007; Constance E. Bagley și Gavin Clarkson, *Adverse Possession for Intellectual Property: Adapting an Ancient Concept to Resolve Conflicts Between Antitrust and Intellectual Property Laws in the Information Age*, Harvard Journal Of Law & Technology, Vol. 16, No. 2, Spring, 2003.

[361] Vezi, spre exemplu, Microsoft Corp. v. Motorola, Inc., 696 F.3d 872 (9th Cir. 2012); Ilor v. Google (Fed. Cir., 2011); Cordance Corp. v. Amazon. com, Inc., 631 F. Supp. 2d 484 (D. Del. 2009); Microsoft Corp. v. AT&T Corp., 550 U.S. 437 (2007); z4 Techs., Inc. v. Microsoft Corp., 434 F. Supp. 2d 437 (E.D. Tex. 2006); eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388 (2006). A se vedea și discuția din Warunee Srisiri-Sisson, *An Extraordinary Decade: The Supreme Court Takes Charge of Reshaping Patent Law*, Charleston Law Review, Vol. 4, 2010.

[362] Vezi Peter Lee, *Patent Law and the Two Cultures*, Yale Law Journal, 120, 2010.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

aceasta[363], unii analişti din domeniu susţinând chiar că dreptul patentelor, în forma sa actuală, este depăşit[364]. Mai mult, numărul mare de aplicaţii pentru acordarea unui brevet de invenţie poate influenţa negativ calitatea patentelor acordate[365] şi duce la întârzieri semnificative în acordarea acestora[366], ceea ce poate crea incertitudine şi complicaţii suplimentare în domeniul atât de dinamic al tehnologiilor avansate.

Brevetele de invenţie constituie, de regulă, cel mai important activ intangibil al unei companii[367], fapt evident în mod deosebit în domeniul tehnologiilor informaţiei şi comunicaţiei[368], domeniu care susţine creşterea tuturor sectoarelor economice şi care este caracterizat de o dinamică deosebită, o competitivitate foarte ridicată[369] şi de investiţii masive în cercetare şi dezvoltare. Pentru a rămâne competitive, firmele din domeniul tehnologiilor informaţiei şi comunicaţiei dezvoltă un portofoliu de patente impresionant. Astfel, IBM, între 1993-2012, a obţinut circa 67.000 patente în SUA (dintre acestea, 6478 doar în 2012), iar Microsoft are circa 49.000 patente la nivel internaţional[370]. Creşterea numărului patentelor din domeniul tehnologiilor informaţiei şi comunicaţiei este foarte semnificativă şi constantă[371]. Având în vedere importanţa patentelor în domeniul tehnologiilor informaţiei şi

363 Vezi Christopher A. Cotropia şi James Gibso, *The Upside of Intellectual Property's Downside*, 57 UCLA Law Review 921, 2010; John M. Golden, *Innovation Dynamics, Patents, and Dynamic-Elasticity Tests for the Promotion of Progress*, Harvard Journal of Law & Technology, Vol. 24, No. 1, Fall, 2010; Matthew Sag, Tonja Jacobi şi Maxim Sytch, *Ideology and Exceptionalism in Intellectual Property: An Empirical Study*, california law review, Vol. 97, 2009.

364 Vezi, spre exemplu, Anna Mancini, *International Patent Law is Obsolete*, 2006. Vezi şi încercări de reformare a sistemului: *The Patent Reform Act of 2011* (S. 23), introdusă în Senatul american în 25 ianuarie 2011 (judiciary.senate.gov/legislation/upload/BillText-PatentReformAct.pdf).

365 Peste 1,2 milioane, conform statisticilor oficiale; vezi o discuţie pe această temă în Jeffrey M. Kuhn, *Information Overload at the U.S. Patent and Trademark Office: Reframing the Duty of Disclosure in Patent Law as a Search and Filter Problem*, 13 Yale Journal of Law & Technology, 90, 2010.

366 Conform *Patent Pendency Statistics* (2009), pentru Computer Architecture, Software & Information Security durata medie de acordare a unui patent este de 40,7 luni - vezi http://www.uspto.gov/patents/stats/patentpendency.jsp.

367 Vezi Malcolm T. Meeks şi Charles A. Eldering, *Patent Valuation: Aren't We Forgetting Something? Making the Case for Claims Analysis in Patent Valuation by Proposing a Patent Valuation Method and a Patent-Specific Discount Rate Using the CAPM*, northwestern journal of technology and intellectual property, Vol. 9, 2010.

368 Conform Nomenclatorului general de activităţi în UE, tehnologiile informaţiei şi comunicaţiei includ cinci clase (sub-sectoare): trei sub-sectoare de manufactură (echipament informatic; componente informatice, telecomunicaţii şi echipament multimedia; instrumente de măsură) şi două sub-sectoare de servicii (servicii de telecomunicaţii; servicii pentru calculatoare şi programe informatice) - vezi în *The 2010 Report on R&D in ICT in the European Union*.

369 Vezi, spre exemplu, mulţimea de sisteme de operare aflate în competiţie: Android, iOS 4, webOS, Symbian, BlackBerry OS 6, QNX, Bada şi Windows 7.

370 Vezi datele prezentate la http://www.research.ibm.com/articles/patents.shtml; http://www.microsoft.com/en-us/legal/intellectualproperty/Patents/Default.aspx?mstLocPickShow=False.

371 O rată anuală de circa 4.7% - vezi OECD, *Compendium of Patent Statistics*, 2008.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

comunicației, disputele legale sunt frecvente[372] și pot implica sume foarte mari, fie că sunt atribuite în instanță[373] sau rezolvate amiabil[374].

Disputelor privind patentele din domeniul tehnologiilor informației și comunicației sunt complicate și complexe și datorită faptului că o singură tehnologie sau produs poate incorpora sute de tehnologii patentate (spre exemplu, video, audio, conectivitate etc.). Firmele producătoare de echipamente sau programe informatice au nevoie, în unele cazuri, de acces la mii de patente pentru a produce un produs comercial[375]. Cele mai disputate patente din domeniul tehnologiilor informației și comunicației privesc programele informatice[376], iar printre aspectele cele mai interesante se numără validitatea unui patent[377], epuizarea unui patent (*patent exhaustion*)[378] și conținutul cererilor unui patent (care prevăd ceea ce nu este permis, fără acordul deținătorului patentului)[379].

---

372 Vezi, spre exemplu, lista disputelor privind *Android* din anul 2010: Apple v. HTC, Oracle v. Google, Interval Licensing v. Google ș.a., Microsoft v. Motorola, Apple v. Motorola, Gemalto v. Google, Samsung, Motorola și HTC, Vertical Computer Systems v. Samsung și LG, Helferich Patent Licensing v. Huawei, Multimedia Patent Trust (Alcatel-Lucent) v. LG ș.a., Hybrid Audio v. HTC, Dell ș.a., Hopewell Culture & Design v. Motorola, Samsung, HTC, LG ș.a., Sony vs. LG).

373 Cele mai mari sume sunt acordate în disputele privind sectorul telecomunicațiilor și al programelor informatice – vezi PricewaterhouseCoopers, *A closer look, 2008 Patent Litigation Study: Damages awards, success rates and time-to-trial* (2008). Vezi, spre exemplu, cazul Mirror Worlds, LLC v. Apple, Inc. (08-CV-88), în care juriul a acordat, în octombrie 2010, despăgubiri de 625,5 milioane dolari pentru încălcarea unor patente; Lucent Technologies, Inc. v. Gateway, Inc. 470 F.Supp.2d 1180 (S.D.Cal., 2007), în care Alcatel-Lucent a primit daune în valoare de 1,53 miliarde dolari (reversat la apel în septembrie 2009).

374 Vezi, spre exemplu, cazul Intel Corporation, care a încheiat disputele legale cu Nvidia Corporation pentru 1,5 miliarde dolari (http://newsroom.intel.com/community/intel_newsroom/blog/2011/01/10/intel-announces-new-patent-cross-license-agreement-with-nvidia).

375 Vezi Federal Trade Commission, *To Promote Innovation: The Proper Balance of Competition and Patent Law and Policy*, A Report by the Federal Trade Commission, 2003.

376 Vezi John R. Allison, Mark A. Lemley și Joshua Walker, *Extreme Value or Trolls on Top? The Characteristics of the Most-Litigated Patents*, University of Pennsylvania Law Review, Vol. 158, 2009. O căutare a autorilor pe Loislaw "patent AND software" pentru întregul an 2010 (*All Federal, Published Opinions*) a generat 412 intrări (401 pentru întregul an 2009, 436 pentru întregul an 2008).

377 Vezi, spre exemplu, *1-Click* (numit și *one-click* sau *one-click buying*), o tehnică ce permite clienților să realizeze cumpărături cu un singu click, dacă informația privind instrumentul de plată este în sistem. *United States Patent and Trademark Office* a acordat Amazon.com în September 1999 patentul număr 5960411 pentru această tehnică. Acest patent a fost reexaminat, iar în martie 2010 a fost confirmat. Solicitarea de reexaminare a unui patent devine, din ce în ce mai mult, o modalitate prin care firmele acuzate de încălcarea unui patent, încearcă să reducă intensitatea disputei sau să oprească, pentru o perioadă îndelungată, disputa.

378 Vezi, spre exemplu, Quanta Computer, Inc., *et al.*, Petitioners, v. LG Electronics, Inc., decis în 9 iunie 2008 la Supreme Court of the United States, discutat pe larg în Emily Van Vliet, *Quanta and Patent Exhaustion: The Implications of the Supreme Court's Decision in Quanta Computer, Inc. v. LG Electronics, Inc. One Year Later*, MINN. J. L. SCI. & TECH., Vol. 11 (2010); Yina Dong, *A Patent Exhaustion Exposition: Situating Quanta v. LGE in the Context of Supreme Court Jurisprudence*, Stanford Technology Law Review, 2010; Tod Michael Leaven, *The Misinterpretation of the Patent Exhaustion Doctrine and the Transgenic Seed*

BUCHAREST CENTRAL UNIVERSITY LIBRARY

Cadrul legal

Sistemul patentelor a fost creat pentru a promova dezvoltarea tehnologică, transferul de tehnologie şi fluxul investiţiilor private. Protecţia patentelor la nivel internaţional începe cu Convenţia de la Paris (*Convention for the Protection of Industrial Property*, 1883). Aceasta a fost urmată de *Patent Cooperation Treaty* (tratat multilateral administrat de OMPI; conform acestuia, un aplicant poate completa o singură aplicaţie de patent internaţională care are aceeaşi valoare ca o aplicaţie naţională), *Strasbourg Agreement Concerning the International Patent Classification* din anul 1971 (sistem de clasificare ierarhică administrat de OMPI în care tehnologia este divizată în secţiuni, clase, subclase şi grupuri, în total circa 70000 de subdiviziuni), *Patent Law Treaty* (care urmăreşte armonizarea şi simplificarea procedurilor formale cu privire la aplicaţiile de patente naţionale sau regionale) şi *Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS Agreement, care stabileşte standarde privind disponibilitatea, domeniul şi folosirea drepturilor privind patentele). Adiţional, un număr de acorduri regionale au contribuit la dezvoltarea sistemului internaţional de patente: *European Patent Convention* şi legislaţia UE, *Eurasian Patent Convention*, *Harare Protocol*, *Bangui Agreement*, *Patent Regulation of the Cooperation Council for the Arab States of the Gulf* şi *Decision 486* (privind state din zona munţilor Anzi).

În România, legislaţia privind brevetele de invenţie include Legea nr. 83/2014 privind invenţiile de serviciu, publicată în Monitorul Oficial, partea I, nr. 471/2014; Legea nr. 64 din 11 octombrie 1991 (republicată) privind brevetele de invenţie), publicată în Monitorul Oficial nr. 541 din 8 august 2007; H.G. nr. 547 pentru aprobarea regulamentului de aplicare a Legii 64/1991 privind brevetele de invenţie, publicată în Monitorul Oficial nr. 456/18 iunie 2008; Legea nr. 611 din 13 noiembrie 2002 privind aderarea României la Convenţia privind eliberarea brevetelor europene, adoptată la Munchen la 5 octombrie 1973, precum şi la Actul de revizuire a acesteia, adoptat la Munchen la 29 noiembrie 2000; Ordinul nr. 112 / 21.11.2008 pentru aprobarea instrucţiunilor privind depunerea cererilor de brevet de invenţie prin mijloace electronice, publicat în Monitorul Oficial nr. 864 din 22 decembrie 2001.

În SUA, secţiunile *Title 35* al United States Code guvernează aspectele privind dreptul patentelor. Pentru obţinerea unui patent, invenţiile trebuie să îndeplinească criteriul privind noutatea (*novelty*), să reprezinte o dezvoltare în domeniu (*inventive step*), să nu fie evidente (*non-obviousness*) şi să fie capabile de folosire industrială (*usefulness*). Sistemul de clasificare al patentelor (*United States Patent Classification* - USPC) este stabilit de către *United States Patent and Trademark Office*. USPC conţine peste 400 de clase, fiecare având un titlu

---

Industry in Light of Quanta V. LG Electronics, North Carolina Journal of Law & Technology, Vol. 10, 1, Fall, 2008.

[379] Vezi, spre exemplu, Mark A. Lemley, *The Changing Meaning of Patent Claim Terms*, 104 Michigan Law Review, 2005 ("The claims of a patent are central to virtually every aspect of patent law"); Tun-Jen Chiang, *Fixing Patent Boundaries*, Michigan Law Review, Vol. 108, February, 2010.

BCU IASI CENTRAL UNIVERSITY LIBRARY

descriptiv şi fiind identificată printr-un număr de clasă. Fiecare clasă este subdivizată în subclase, identificate printr-un număr de subclasă.

Încălcarea unui patent este comiterea unui act interzis fără a avea permisiunea deţinătorului patentului (de regulă, acordată sub forma unei licenţe). Fabricarea, importarea, folosirea, vânzarea sau oferirea spre vânzare de tehnologie patentată sunt considerate încălcare a patentului. Patentele sunt teritoriale, încălcarea acestora fiind posibilă doar în ţara în care patentul este valid.

Cazuri[380]

i4i Limited Partnership v. Microsoft Corp.[381]

În martie 2007, i4i a acţionat în instanţă corporaţia Microsoft pentru încălcarea patentului No. 5,787,449 (*Method and System for Manipulating the Architecture and the Content of a Document Separately from Each Other*) prin fabricarea, vânzarea şi/sau importul produselor Word 2003 şi Word 2007, conform 35 U.S.C. § 284. Patentul în cauză este un sistem/metodă gândită pentru programatori, pentru manipularea separată a arhitecturii şi conţinutului unui document, în special pentru reprezetarea şi transformarea datelor, ceea ce permite multiple modalităţi de vizualizarea a conţinutului său prin producerea unui metacod.

În 20 mai 2009, juriul a decis că patentul în cauză este valid şi încălcat de Microsoft, acordând daune pentru i4i. În august 2009, judecătorul din acest caz a acordat daune ce depăşesc 290 milioane dolari pentru i4i şi o *permanent injunction* împotriva corporaţiei Microsoft. Microsoft a făcut apel în Federal Circuit Court of Appeals la sfârşitul anului 2009, dar fără success. *United States Patent and Trademark Office* a reafirmat validitatea patentului în cauză, iar la sfârşitul anului 2010 a refuzat o nouă cerere a Microsoft pentru re-examinarea patentului. În noiembrie 2010, Curtea Supremă a SUA a acceptat să judece acest caz[382], şi, în iunie 2011, a dat câştig de cauză pentru i4i, Microsoft trebuind să plătească daune de 290 milioane de dolari către i4i.

Bid for Position, LLC v. AOL, LLC[383]

În aprilie 2010, Federal Circuit a afirmat decizia curţii districtuale privind sistemul de reclame al Google numit AdWords, considerând că acesta nu încalcă patentul No. 7,225,151 (*Online Auction Bid Management System and Method*), care se referă la o metodă sau sistem pentru administrarea automată a unei licitaţii pe Internet pentru a determina priorităţi relative, bazate pe valoarea licitată (programul AdWords este folosit pentru determinarea de poziţii pentru afişarea de reclame pe Internet). Acest caz ilustrează riscul ca unele patente, în special cele

---

380 Toate patentele menţionate în această secţiune au fost acordate de United States Patent and and Trademark Office.

381 Vezi i4i Ltd. Partnership v. Microsoft Corp., 598 F.3d 831 (Fed. Cir. 2010); i4i Limited Partnership v. Microsoft Corp., 07-CV-00113-LED (E.D. Tex, 2009).

382 Microsoft Corp. v. i4i Ltd. Partnership, No. 10-290 (U.S. June 9, 2011).

383 Bid for Position, LLC v. AOL, LLC, 601 F.3d 1311 (Fed. Cir., 2010).

BCU IASI / CENTRAL UNIVERSITY LIBRARY

privind programe informatice şi metode de realizarea a afacerilor electronice, să fie prea abstracte. Instanţa a considerat, în acest caz, că patentul în discuţie se referă doar la licitaţii similare celor descrise în aplicaţia patentului.

3.3.2.2 Topografia produselor semiconductoare

Un *circuit integrat*, cunoscut şi sub denumiri cum ar fi *IC*, *microcircuit*, *microcip* sau *cip de silicon*, este un dispozitiv electronic miniaturizat, fabricat în suprafaţa unui strat de material semiconductor, de obicei siliciu[384], care conţine o combinaţie de elemente interconectate, asociate inseparabil. Circuitele integrate digitale pot conţine multe milioane de porţi logice[385], circuite *flip-flop*[386], multiplexoare[387] şi alte circuite dispuse pe câţiva milimetri pătraţi şi sunt compuse din multe straturi sau nivele suprapuse (nivel de *difuzare*, *implant*, *polysilicon* sau *metal*, *via* sau *contact*), fiecare definit de fotolitografie[388] şi realizat în culori diferite[389]. Datorită proprietăţilor materialelor folosite, circuitele integrate sunt numite şi produse semiconductoare.

Circuitele integrate au devenit parte esenţială a calculatoarelor, telefoanelor celulare şi a altor echipamente electronice, pe bună dreptate considerându-se că revoluţia digitală declanşată de acestea este una dintre cele mai importante în istoria umanităţii. Primele circuite integrate au fost realizate independent de Jack Kilby de la Texas Instruments în anul 1959 şi Robert Noyce de la Fairchild Semiconductor în anul 1961. Primele circuite integrate numărau câteva zeci de tranzistori şi au fost numite *Small-Scale Integration* (SSI). Următorul pas în dezvoltarea circuitelor integrate a avut loc la sfârşitul anilor '60, când au apărut aşa-numitele *Medium-Scale Integration* (MSI), care conţineau sute de tranzistori şi prezentau un număr de avantaje faţă de circuitele din generaţia anterioară. La jumătatea anilor '70 a apărut generaţia *Large-Scale Integration* (LSI) cu zeci de mii de tranzistori pe cip. Următorul nivel a fost reprezentat, începând din anii '80, de *Very-Large-Scale Integration* (VLSI), în anul 1986 primul cip RAM de 1 megabit conţinea peste 1 milion de tranzistori. Pentru a reflecta complexitatea circuitelor integrate din zilele noastre – care conţin câteva zeci de miliarde de tranzistori - a fost propus termenul *Ultra-Large-Scale Integration* (ULSI).

Circuitele integrate cuprind o gamă largă de produse, cum ar fi microprocesoare, memorii dinamice etc. Printre cele mai importante firme care

---

384 Mai rar alte materiale, cum ar fi, spre exemplu, germaniu.

385 Circuit cu unul sau mai multe intrări (*input*) şi o ieşire (*output*). Cele patru tipuri de porţi sunt numite AND (rezultatul este adevărat doar dacă toate intrările sunt adevărate), OR (rezultatul este adevărat dacă cel puţin una dintre intrări este adevărată), NAND (rezultatul este fals doar dacă toate intrările sunt adevărate, altfel rezultatul este adevărat) şi NOR (rezultatul este fals dacă cel puţin una dintre intrări este falsă şi adevărat dacă toate intrările sunt false).

386 Cale conductivă care are două condiţii de stabilitate permanentă şi o modalitate de schimbare de la una la alta ca răspuns la un stimul extern.

387 Pentru transmiterea a două sau mai multe mesaje simultan pe un singur canal de transmisie.

388 Tehnică de fabricaţie a circuitelor integrate, care constă în crearea de părţi oxidate pe suprafaţa unui cip de siliciu expus la ultraviolete.

389 Toate componentele fiind realizate prin combinarea specifică a acestor straturi.

fabrică asemenea produse se numără Alcatel, Altera, AMD, ATI Technologies, Fujitsu, Hitachi, Infineon Technologies, Intel, Lattice Semiconductor, Linear Technology, NEC Electronics, Silicon Optix, STMicroelectronics, Texas Instruments, Toshiba, VIA Technologies, Vitesse Semiconductor, Volterra Semiconductor, Xilinx, ZiLOG etc. Deoarece complexitatea produselor semiconductoare depinde în principal de conceperea topografiilor de produse semiconductoare, realizarea acestora fiind, cel mai adesea, foarte complexă și costisitoare, a apărut necesitatea protecției acestora.

Protecția internațională

Deși pe plan internațional dispute în acest domeniu sunt rare[390], pentru protejarea creativității și a investițiilor implicate în realizarea topografiilor produselor semiconductoare, la nivel internațional s-a încercat introducerea unei protecții globale a topografiilor circuitelor integrate[391]. Conform *Treaty on Intellectual Property in respect of Integrated Circuits*[392] (Washington, 26 Mai 1989), prin "circuit integrat" se înțelege un produs în formă finală sau intermediară, în care elementele, dintre care cel puțin unul este un element activ[393], iar unele sau toate interconexiunile sunt formate integral în și/sau pe o bucată de material și care execută o funcție electronică [Art. 2(i)]. Prin "topografie" (*layout design*) se înțelege dispoziția tri-dimensională, indiferent cum este ea exprimată, a elementelor componente [Art. 2(ii)].

Art. 6.1 al *Treaty* enumeră actele care solicită autorizarea titularului: reproducerea totală sau parțială prin incorporarea într-un circuit integrat, importul, vânzarea sau distribuirea pentru scopuri comerciale. Acordul TRIPS (*Trade Related Intellectual Property Rights*)[394], prin articolele 35–38 oferă, de asemenea, provizii pentru protecția topografiilor folosite în circuitele integrate [*Section 6 – Layout-Designs (Topographies) of Integrated Circuits*].

Directiva Consiliului European 87/54/EEC din 16 Decembrie 1986 [*on the Legal Protection of Topographies of Semiconductor Products*, 1987 O.J. (L 24) 36], a obligat statele membre să adopte legi care să oferă o protecție adecvată topografiilor produselor semiconductoare. Conform Directivei, prin "topografie" se înțelege o serie de imagini, fixate sau codate, care (i) reprezintă modelul tri-dimensional ale straturilor din care este compus produsul semiconductor și (ii) în care fiecare imagine are un model sau parte a modelului unei suprafețe a produsului semiconductor la orice etapă a fabricării (Article 1). O topografie este

---

390 Vezi în SUA, spre exemplu, *Brooktree Corp. v. Advanced Micro Devices Inc* (977 F2d. 1555, Fed. Circ. 1992), în M. Lemley, P. Menell, R. Merges și P. Samuelson, *Software and Internet Law*, 2000.

391 Vezi, spre exemplu, P. K. Yu, *Five Disharmonizing Trends in the International Intellectual Property Regime*, 2006; T. Hoeren, *Chip Protection in Europe*, 2003.

392 Tratatul a fost adoptat în anul 1989, dar nu a fost ratificat niciodată – vezi detalii în C. R. Romițan, *Protecția penală a proprietății intelectuale*, Ed. C.H. Beck, București, 2006, p. 255.

393 Componentele active sunt elemente într-un circuit care măresc puterea sau multiplică fluxul curent. Componentele active rectifică, amplifică și comută, spre deosebire de componentele pasive (rezistorii, inductori, capacitori și interconexiunile).

394 Realizat în 15 April 1994, în vigoare din 1 Januarie 1995.

BOLYAI/CENTRAL UNIVERSITY LIBRARY

protejabilă dacă este rezultatul efortului intelectual al creatorului şi nu este uzuală în industria produselor semiconductoare (Art. 2).

Protecția topografiilor în România

În România, Legea nr. 16 din 6 martie 1995[395] priveşte protecţia topografiilor circuitelor integrate[396]. Această lege a fost modificată de Legea nr. 337/2005 privind protecţia produselor semiconductoare[397]. Produsele semiconductoare sunt protejabile prin înregistrare la Oficiul de Stat pentru Invenţii şi Mărci, în condiţiile prevăzute de lege (Art. 1).

"Produs semiconductor" este forma finală sau intermediară a oricărui produs:

- compus dintr-un substrat ce comportă un strat de material semiconductor; şi
- constituit din unul sau mai multe straturi de materiale conductoare, izolante ori semiconductoare, straturile fiind dispuse conform unei configuraţii tridimensionale prestabilite; şi
- destinat să îndeplinească, în mod exclusiv sau nu, o funcţie electronică.

"Topografie a unui produs semiconductor" este o serie de imagini legate între ele, indiferent de modalitatea în care acestea sunt fixate sau codate, reprezentând configuraţia tridimensională a straturilor care compun un produs semiconductor şi în care fiecare imagine reproduce desenul sau o parte din desenul unei suprafeţe a produsului semiconductor, în orice stadiu al fabricaţiei sale. Sunt considerate originale şi protejabile topografiile care "constituie rezultatul efortului intelectual al creatorilor lor şi care, la data când au fost create, nu erau uzuale pentru creatorii de topografii şi pentru fabricanţii de produse semiconductoare". O topografie constituită dintr-o combinaţie de elemente şi de interconexiuni uzuale poate fi protejată "numai dacă combinaţia, luată în ansambul ei, este originală".

Drepturile titularului unei topografii protejate asupra produsului semiconductor nu sunt condiţionate de faptul că acesta este sau nu încorporat într-un produs. Protecţia se aplică numai topografiei propriu-zise, cu "excluderea oricărui concept, procedeu, sistem, tehnici sau informaţii codate încorporate în topografie". Conform Art. 50 din Legea nr. 187/2012, care modifică art. 38 al Legii nr. 16/1995, "exploatarea comercială sau producerea fără drept a unei topografii protejate ori a unui produs semiconductor în care este încorporată o topografie protejată sau a unui element de circuit care încorporează un astfel de produs semiconductor, în măsura în care acest element continuă să conţină o topografie, dacă fapta a fost comisă după data publicării înregistrării topografiei în Registrul naţional al topografiilor, constituie infracţiunea de contrafacere şi se

---

395 Textul actului a fost publicat în M.Of. nr. 45/9 martie 1995, republicat în temeiul art. III din Legea nr. 337/2005 pentru modificarea şi completarea Legii nr. 16/1995 privind protecţia topografiilor circuitelor integrate. Legea a mai fost modificată şi completată prin alte acte normative, vezi http://www.cdep.ro/pls/legis/legis_pck.htp_act?ida=6628.

396 Topografiile produselor semiconductoare conform Legii nr. 337 din 29 noiembrie 2005 pentru modificarea şi completarea Legii nr. 16/1995.

397 Din 29 noiembrie 2005, textul actului publicat în M.Of. nr. 1094/5 decembrie 2005.

pedepseşte cu închisoare de la 3 luni la 2 ani sau cu amendă". Asemenea acţiuni sunt calificate contrafacere dacă au fost săvârşite după data publicării înregistrării topografiei în Registrul naţional al topografiilor şi se pedepsesc cu închisoare sau cu amendă, iar acţiunea penală se pune în mişcare din oficiu[398].

Pentru prejudiciile cauzate, titularul are dreptul la despăgubiri şi poate solicita instanţei judecătoreşti competente să dispună măsura confiscării sau, după caz, a distrugerii produselor contrafăcute. Aceste dispoziţii se aplică şi echipamentelor care au servit nemijlocit la săvârşirea infracţiunii de contrafacere.

3.3.2.3 Secrete comerciale

Prin "secret comercial" se înţelege, în general, o informaţie valoroasă, sau potenţial valoroasă, pe care deţinătorul încearcă să o păstreze secretă prin intermediul unor contracte de confidenţialitate cu angajaţi, contractanţi sau parteneri şi/sau prin intermediul unor măsuri de securitate fizică şi/sau electronic (cum ar fi criptare, autentificare, controlul accesului, marcarea "confidenţial" sau "secret" a documentelor etc.), astfel încât singurul mod în care secretul comercial poate fi divulgat (făcut cunoscut unor terţe părţi) este prin intermediul încălcării unui contract sau a unor măsuri de securitate, cu alte cuvinte, prin intermediul unui act de natură penală. Conform Organizaţiei Mondiale a Proprietăţii Intelectuale (WIPO)[399], printre categoriile care pot fi considerate secrete comerciale se numără:

- Compilaţii de date (spre exemplu, liste de clienţi);
- Desene, planuri arhitecturale sau hărţi;
- Programe informatice[400];
- Algoritmi şi procese care sunt implementate în alte programe informatice;
- Metode instrucţionale;
- Procese, tehnici şi *know-how* de producţie sau reparare;
- Procese de urmărire a documentelor;
- Formule sau ingrediente pentru fabricarea unor produse[401];
- Strategii sau planuri de afaceri sau marketing;
- Informaţii financiare;
- Informaţii privind personalul angajat;
- Planificări;
- Manuale;
- Informaţii despre activităti de cercetare sau dezvoltare.

---

398 Vezi Ordonanţa de Urgenţă nr. 190 din 21 noiembrie 2005.

399 Vezi WIPO Magazine, *Trade secrets are gold nuggets: Protect them*, April, 2002.

400 Spre exemplu, un program informatic folosit în industria forestieră – vezi cazul Rivendell Forest Prods., Ltd. v. Georgia-Pacific Corp., 28 F.3d 1042, 1046 (10th Cir. 1994).

401 Spre exemplu, reţeta Coca-Cola, cunoscută doar de două persoane, ale căror nume sunt păstrate secret (singura descriere în scris a reţetei este păstrată într-un seif bancar, care poate fi deschis numai printr-o rezoluţie a Board of Directors), dar şi reţete pentru pizza, spre exemplu - vezi cazul Magistro v. J. Lou, Inc., 703 N.W.2d 887, 890-91 (Neb. 2005).

Protecţia secretelor comerciale este o componentă importantă în cadrul protecţiei investiţiilor din domeniul proprietăţii intelectuale[402]. Nu există date exacte privind valoarea secretelor comerciale, cu toate acestea economiştii estimează că acestea reprezintă un procent important şi în continuă creştere din proprietatea intelectuală (estimată, în SUA, la cinci trilioane dolari)[403]. Cercetătorii estimează că secretele comericale acoperă peste 90% din tehnologiile noi şi că peste 80% licenţe şi convenţiile de transfer de tehnologie implică secrete comerciale sau constituie o înţelegere hibridă privind patentele şi secretele comerciale[404].

Secretele comerciale pot reprezenta un procent semnificativ din activele (*assets*) unei companii[405], în unele cazuri putându-se vorbi de furtul unor secrete comerciale în valoare de un miliard de dolari[406]. În SUA, există sute de decizii în instanţe federale în fiecare an privind secretele comerciale, iar numărul acestor cazuri continuă să crească[407]. Digitizarea crescândă şi capacitatea de accesare şi diseminare rapidă şi globală oferită de Internet prezintă pericole reale la adresa secretelor comerciale[408].

Domeniul tehnologiei informaţii prezintă numeroase cazuri de încălcare a secretelor comerciale şi reprezintă un subiect important în cadrul cercetării din domeniu[409], o atenţie deosebită fiind acordată modului în care poate fi divulgarea secretelor comerciale poate fi împiedicată sau limitată în cazul unor angajaţi care

---

402 Vezi C. R. J. Pace, *The case for a federal trade secrets act*, Harvard Journal of Law and Technology, Vol. 8 (2), 1995.

403 Vezi D. S. Almeling şi colab., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, Gonzaga Law Review, Vol. 45, 2010.

404 Vezi J. Mazzone şi M. Moore, op. cit.

405 Vezi J. P. Hutchins, *The Corporation's Valuable Assets: IP Rights Under Sox*, 26TH Annual Institute On Computer & Internet Law 289, 291 (PLI Intellectual Property, Course Handbook Series No. G-859), 2006.

406 Spre exemplu, cazul în care Biswamohan Pani a fost acuzat că a furat, de la firma Intel, în noiembrie 2008, secrete comerciale în valoare de un miliard de dolari – vezi detalii la http://www.networkworld.com/news/2008/110608-intel-trade-secrets-theft-indictment.html ?ts0hb&story=ts_whsp şi http://spectrum.ieee.org/semiconductors/processors/lessons-from-the-1-billion-intel-tradesecret-theft. În Almeling şi colab., op. cit., se vorbeşte despre un cost anualizat al furturilor din acest domeniu, doar în SUA, de circa 300 miliarde dolari.

407 Vezi Almeling şi colab., op. cit. O căutare "trade secret" pe Loislaw a autorilor pentru luna Octombrie 2010 a afişat 153 cazuri, pentru anul 2010 (până la sfârşitul lui Octombrie) a afişat 924 cazuri, iar pentru anul 2005 a afişat 695 cazuri.

408 Vezi discuţii pe această temă în V. A. Cundiff, *Reasonable measures to protect trade secrets in a digital environment*, IDEA - The Intellectual Property Law Review, Vol. 49 (3), 2009; A. Beckerman-Rodau, *Trade secrets – The new risks to trade secrets posed by computerization*, Rutgers Computer & Technology Law Journal, Vol. 28 (2002); E. A. Rowe, *Introducing a takedown for trade secrets on the Internet*, Wisconsin Law Review, 2007.

409 Vezi, spre exemplu, E. A. Rowe, *Trade secret litigation and free speech: is it time to restrain the plaintiffs?*, Boston College Law Review, Vol. 50, 2009; P. Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 Hastings Law Journal 777, 805–08, 2007; M. L. Rustad, *Negligent Enablement of Trade Secret Misappropriation*, 22 Santa Clara Computer & High Technology Law Journal 455, 2006.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

pleacă[410]. Conform unui studiu, în peste 85% din cazurile din domeniul secretelor comerciale, persoana care a obținut fără drept un secret comercial a fost fie un angajat, fie un partener de afaceri[411].

Spre deosebire de patente sau drepturi de autor, care necesită un grad ridicat de noutate, secretele comerciale trebuie să prezinte o noutate "minimală". Mai mult, un secret comercial poate include elemente care sunt în domeniul public, dacă secretul comercial în sine constituie o integrare unică, efectivă și valoroasă a elementelor din domeniul public[412]. Brevetele de invenție și secretele comerciale nu sunt incompatible, ci se completează, ultimele protejând *know-how* colateral asociat cu patente[413].

În **SUA**, legislația secretelor comerciale este statală, fiecare stat determinând individual modul de protecție al acestora. În cadrul statelor, dreptul secretelor comerciale își are originea în *common law*[414]. Cea mai larg acceptată și citată definiție a secretelor comerciale poate fi găsită în *Restatement (First) of Torts*. Astfel, un "secret comercial" poate consta din orice formulă, patern, dispozitiv sau compilație de informații care este folosită în cadrul activităților comerciale ale unei forme și care îi oferă ocazia de a obține un avantaj în fața competitorilor care nu îl cunosc sau nu îl folosesc.

Foarte important în USA este *Uniform Trade Secrets Act* (UTSA)[415], adoptat de 46 state, District of Columbia și U.S. Virgin Islands. Conform UTSA, un "secret comercial" este informație, inclusive o formulă, patern, compilație, program, dispozitiv, metodă, tehnică sau process care:

(i) Furnizează valoare economică, actual sau potențială, din faptul că nu este cunoscut de alții și nu poate fi obținut prin mijloace acceptabile de către alte entități care pot obține o valoare economică din divulgarea sau folosirea sa,

(ii) Este subiectul unor eforturi rezonabile de menținerea a secretului său.

Un altă reglementare legală esențială în cadrul protecției secretelor comerciale este *Economic Espionage Act*[416] (EEA). Conform EEA, un "secret comerical" înseamnă toate formele și tipurile de informații financiare, de afaceri, științifice, tehnice, economice sau inginerești, incluzând forme, planuri, compilații, dispozitive, formule, desene, prototipuri, metode, tehnici, procese, proceduri, programe, tangibile sau intangibile, stocate, compilate, memorate fizic, electronic,

---

410 Vezi o discuție largă pe această temă în R. S. Arnow-Richman, *Bargaining for Loyalty in the Information Age: A Reconsideration of the Role of Substantive Fairness in Enforcing Employee Noncompetes*, Oregon Law Review, Vol. 80 (4), 2001; vezi și V. A. Cundiff, op. cit. și cazul Mattel, Inc. v. MGA Entertainment, Inc., 09-55673 (9th Cir. 7-22-2010).

411 Vezi D. S. Almeling și colab., op. cit.

412 Vezi, în acest sens, *Theft of Commercial Trade Secrets* - 18 U.S.C. §§ 1831-1839.

413 Vezi, în acest sens, Karl F. Jorda, *Patent and Trade Secret Complementariness: An Unsuspected Synergy*, Washburn Law Journal, Vol. 48, 2008.

414 Vezi Jason Mazzone și Matthew Moore, op. cit.

415 Uniform Trade Secrets Act §§ 1-12, 14 U.L.A. 437-467 (1990 & Supp. 1993). Vezi o discuție extinsă despre UTSA în Jason Mazzone și Matthew Moore, op. cit.; Miles J. Feldman, *Toward a clearer standard of protectable information: trade secrets and the employment relationship*, Berkeley Technology Law Journal, 2005.

416 18 U.S.C. § 1831 (1996).

geographic fotografic sau în scris sau nu, dacă:

(i) Deţinătorul a luat măsuri rezonabile pentru a păstra informaţia secretă şi

(ii) Informaţia permite obţinerea unei valori economice independente, actuale sau potenţiale, din faptul că nu este cunoscută sau uşor de obţinut prin mijloace legale de public[417].

"Secretele comerciale" sunt protejate în **România** prin Legea privind combaterea concurenţei neloiale, nr. 11/1991, modificată şi completată prin Ordonanţa Guvernului nr. 12/2014, actualizată în ianuarie 2005 (modificată şi completată prin Legea concurenţei nr. 21/1996, completată şi modificată prin Legea nr. 298/2001). Ordonanţa Guvernului nr. 12/2014 pentru modificarea şi completarea Legii nr. 11/1991 privind combaterea concurentei neloiale şi a altor acte în domeniul protectiei concurentei a fost publicata in Monitorul Oficial, Partea I, nr. 586 din 6 august 2014. Constituie "secret comercial" orice *informaţie care, total sau parţial, nu este în general cunoscută sau nu este uşor accesibilă persoanelor din mediul care se ocupă în mod obişnuit cu acest gen de informaţie şi care dobândeste o valoare comercială prin faptul că este secretă, pentru care deţinătorul legitim a luat măsuri rezonabile ţinând seama de circumstanţe, pentru a fi mentinută în regim de secret; protecţia secretului comercial operează atât timp cât condiţiile enunţate anterior sunt îndeplinite în mod cumulativ.*

Este considerată ca fiind contrară uzanţelor comerciale cinstite utilizarea în mod neloial a secretelor comerciale ale unui comerciant prin practici de genul neexecutării unilaterale a contractului sau utilizării unor proceduri neloiale, abuzului de încredere, incitării la delict şi achiziţionării de secrete comerciale de către terţii care cunoşteau că respectiva achiziţie implică astfel de practici, de natură să afecteze poziţia comercianţilor concurenţi pe piaţă. Încălcarea acestei obligaţi atrage raspundere civilă, contravenţională ori penală.

Cazuri

Hewlett-Packard Company v. Mark V. Hurd[418]

Hewlett-Packard este una dintre firmele cele mai mari şi mai importante din domeniul tehnologiei informaţiei, furnizând produse de vârf în domeniul sistemelor personale, al imprimantelor şi al *Enterprise Business*. Fiind concediat de Hewlett-Packard în 6 august 2010 (în urma terminării contractului Hurd a primit mai multe milioane de dolari şi părţile au reafirmat obligativitatea protecţiei secretelor comerciale), Mark Hurd a acceptat să lucreze pentru Oracle Corporation, un competitor direct al HP.

Mark Hurd a avut poziţii de vârf în cadrul companiei Hewlett-Packard (*Chairman of the Board, Chief Executive Officer* şi *President*) şi a fost responsabil cu crearea planurilor strategice ale companiei şi cu planurile de acţiuni comerciale

---

[417] Vezi o discuţie a tipurilor de obţinere fără drept în *Theft of Commercial Trade Secrets* - 18 U.S.C. §§ 1831-1839.

[418] Superior Court of the State of California, County of Santa Clara, 7 septembrie 2010 - *Demand for injunctive relief and jury trial.*

BCU IASI CENTRAL UNIVERSITY LIBRARY

împotriva firmelor rivale, inclusive a Oracle, firma care l-a angajat pe Hurd după ce a fost demis de Hewlett-Packard (Oracle este o corporaţie cu care, de altfel, Hewlett-Packard colaborează, având circa 140.000 de clienţi comuni). Pentru păstrarea confidenţialităţii informaţiilor la care a avut acces, Hurd a fost plătit cu câteva milioane dolari, acţiuni şi opţiuni de cumpărare acţiuni.

În plângerea civilă, Hewlett-Packard a argumentat că Mark Hurd nu poate lucra pentru Oracle fără a divulga secrete comerciale şi informaţii confidentiale ale Hewlett-Packard şi că acesta încalcă obligaţii legale şi contractuale prin acceptarea poziţiei la Oracle. Acordul de confidenţialitate semnat de Mark Hurd privea secretele comerciale, informaţiile confidenţiale şi tehnice şi *know-how* necunoscute publicului, obţinute sau produse de el în timpul contractului cu Hewlett-Packard.

Informaţiile confidenţiale la care se face referire în Acord pot include, fără limitare, informaţii privind organizarea, structura şi finanţele companiei, performanţa angajaţilor, cercetarea, dezvoltarea, fabricarea, marketingul, certificate, chei, parole şi alte informaţii informatice, precum şi informaţii pe care Hewlett-Packard le primeşte de la alte părţi cu obligaţia de a le păstra confidenţiale. Aceste informaţii puteau fi folosite de Mark Hurd doar ca angajat al Hewlett-Packard, confidenţial şi luând măsuri care să asigure că asemenea informaţii nu sunt divulgate unor persoane neautorizate sau folosite într-o manieră neautorizată, atât în timpul, cât şi după terminarea contractului între părţi.

Prin urmare, în plângerea depusă se solicita ca Mark Hurd să nu fie lăsat în acea poziţie în care el poate utiliza secretele comerciale). Părţile au ajuns la o înţelegere, conform căreia Hurd renunţă la acţiuni în valoare de 14 milioane dolari, pentru a putea lucra pentru Oracle[419].

International Business Machines Corporation v. Mark D. Papermaster[420]

În 2008, Mark Papermaster, Vice-Preşedinte al Blade Development Unit a IBM, a devenit subiectul unei acţiuni legale pentru obţinerea de secrete comerciale şi încălcarea clauzei de *non-compete* (clauză de non-concurenţă neloială), când acesta a anunţat că va lucra pentru firma Apple ca Senior Vice President al Devices Hardware Engineering. IBM a argumentat în plângerea depusă că Papermaster a avut acces la secrete comerciale şi că există un risc ridicat ca acesta să le divulge ca angajat al Apple, în detrimentul IBM.

United States District Court in the Southern District of New York a acordat IBM *motion for preliminary injunctive relief*. Adiţional, judecătorul acestui caz a decis că IBM trebuie să plătească un bond de 3 milioane dolari pentru costuri sau daune pe care Papermaster le-ar putea solicita în timp ce nu poate lucra pentru Apple. În January 2009, s-a anunţat că părţile au ajuns la o înţelegere, în cadrul căreia Papermaster va certifica într-un cadrul legal că protejează secretele comerciale ale IBM.

---

[419] http://finance.yahoo.com/news/HP-Hurd-reach-settlement-over-apf-162022018.html?x=0.
[420] 409 F. Supp. 2d 253, 255 (S.D.N.Y. 2005).

United States v. William P. Genovese, Jr.[421]

În februarie 2004, porţiuni de cod sursă din sistemele de operare Windows NT 4.0 şi Windows 2000, aparţinând firmei Microsoft, au fost oferite pentru vânzare pe Internet (prin intermediul unui server FTP). Microsoft a alertat FBI şi în iulie 2004 un agent sub acoperire l-a contactat pe Genovese şi a cumpărat cod sursă. În ianuarie 2005, William P. Genovese, Jr. a fost condamnat pentru descărcarea (*downloading*) şi vânzarea de secrete comerciale, încălcând astfel prevederile 18 U.S.C. § 1832(a)(2).

În apărarea sa, Genovese a susţinut că definiţia "secretului comercial" este foarte vagă, chiar neconstituţională, aplicată la faptele cazului său şi că prevederile *Economic Espionage Act* violează *First Amendment* (chiar dacă acesta nu protejeză acţiuni prin care se încearcă obţinerea de beneficii economice prin exploatarea unui secret comercial). De asemenea, Genovese a susţinut că el nu putea să ştie că acel cod nu era cunoscut publicului, sau că Microsoft a luat măsuri rezonabile de protejare a acestuia. În acest caz, curtea a susţinut că un secret comercial nu îşi pierde protecţia când, temporar, accidental sau illicit, este făcut cunoscut publicului[422].

3.3.2.3.1 Cod sursă

Datorită valorii reale sau potenţiale, o poziţie specială în cadrul discuţiei despre secrete comerciale este ocupată de *codul sursă* al programelor pentru calculator[423]. Crearea de programe pentru calculator necesită utilizarea unor resurse umane, tehnice şi financiare deosebite, în unele cazuri codul sursă constituind principalul avantaj competitiv pentru firme, obţinerea fără autorizare a codului sursă putând rezulta în pierderea acestui avantaj şi a clienţilor existenţi sau potenţiali. În cazul programelor pentru calculator, secretele comerciale pot lua mai multe forme: funcţionalitatea codului obiect; codul sursă care implementează algoritmi (care pot fi, la rândul lor, secreţi); informaţii sau formule în interiorul codului sursă; algoritmi sau arhitectură informatică; structuri de date[424].

Obţinerea ilegală a codului sursă poate fi realizată cu scopul de a forma o nouă firmă (care se va afla în competiţie cu firma victimă), furnizarea codului unui

---

421 United States v. Genovese, 409 F. Supp. 2d 253 (S.D.N.Y. 2005). Cazul este discutat pe larg în Elizabeth A. Rowe, *Saving trade secret disclosures on the Internet through sequential preservation*, Wake Forest Law Review, Vol. 42, No. 1, 2007.

422 De remarcat, în acest context, că dacă o informaţie postată pe Internet cauzează intrarea acesteia în domeniul public, o persoană care republic acea informaţie nu se face vinovată de obţinerea unui secret comercial, chiar dacă a ştiut că acea informaţia a fost obţinută prin mijloace ilegale – vezi, în acest sens, cazul DVD Copy Control Ass'n Inc. v. Bunner, 10 Cal. Rptr. 3d 185, 194 (Cal. Ct. App. 2004).

423 Vezi, spre exemplu, Michael Hanley, Tyler Dean, Will Schroeder, Matt Houy, Randall F. Trzeciak, Joji Montelibano, *An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases*, 2011. Vezi şi Kurt M. Saunders, *The Law And Ethics Of Trade Secrets: A Case Study*, California Western Law Review, Vol. 42, 2006.

424 Vezi Charles T. Graves şi Brian D. Range, *Identification of Trade Secret Claims in Litigation: Solutions for a Ubiquitous Dispute*, Northwestern Journal of Technology and Intellectual Property, Vol. 5, No. 1, 2006, p. 94.

competitor[425], noului angajator (în unele situații aflat într-o altă țară[426]) sau vânzarea acestuia[427]. Obținerea și folosirea fără autorizare a codului sursă poate duce la procese civile sau penale privind încălcarea dreptului de autor, a secretelor comerciale sau pentru competiție neloială[428]. În această secțiune, ne propunem să prezentăm aspecte teoretice esențiale legate de obținerea și folosirea fără autorizare a codului sursă și cazuri din practica americană.

Codul sursă al unui program pentru calculator (*computer software* sau *computer program*) este textul scris într-un limbaj de programare de nivel înalt[429] (în unele situații conținând și porțiuni scrise în limbaj de asamblare, pentru optimizarea eficienței procesorului[430]). Codul obiect (*object code*, numit și *binaries*) este compilarea codului sursă într-un limbaj înțeles de calculator: șiruri de numere binare sau hexazecimale[431], care nu pot fi înțelese de oameni, obținute prin intermediul unui program special, numit compilator (care execută o analiză lexicală și sintactică a codului sursă, după care generează și optimizează codul obiect)[432]. Altfel spus, codul sursă este materia primă pentru obținerea codului obiect, ceea ce este folosit de compilator pentru a genera codul obiect (instrucțiuni privind modul de compilare putând fi incluse în codul sursă). Codul sursă poate fi conținut în unul sau mai multe fișiere și, în cazul programelor complexe, poate avea câteva milioane de linii (de regulă, este semnificativ mai mare în dimensiuni decât codul obiect).

Codul sursă este independent de platformă, adică nu se referă la un anume tip de calculator (procesor) sau sistem de operare. Codul sursă al unui program pentru calculator poate fi de tip deschis sau public (*free* și *open source software*[433], numite uneori și *freeware* sau *copyleft*, distribuirea acestui cod trebuind să respecte anumite condiții[434]; de remarcat că programele pentru calculator de tip *freeware* nu

---

425 Vezi, spre exemplu, cazul Optionmonster Holdings, Inc. v. Tavant Technologies (N.D.Ill. 6-29-2010) și cazul Meng în US DoJ, *PRO IP Act First Annual Report 2008-2009*, Oct 13, 2009.

426 Vezi, spre exemplu, Derrick Spooner, Dawn M. Cappelli, Andrew P. Moore și Randall F. Trzeciak, *Spotlight On: Insider Theft of Intellectual Property inside the U.S. Involving Foreign Governments or Organizations*, 2009.

427 Vezi Mark L. Krotoski, *Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases*, United States Attorneys' Bulletin, November, 2009. Vezi și cazul *United States v. William P. Genovese, Jr*.

428 Vezi Belinda M. Juran, Michael A. Diener și Benjamin Koch, *Trade Secret Protection for Source Code*, 2001.

429 Exemple de limbaje: C, C++, Fortran, Visual Basic, Java, Perl, PHP, Python, Tcl/Tk etc.

430 Vezi www.linfo.org/source_code.html.

431 Spre exemplu, instruciunea "MOV" pentru un microprocesor Intel pe 32 de biți poate fi reprezentată în cod binar ca "10110000 01100001", iar în cod hexazecinal ca "B0 61" – vezi explicațiile date în Silvaco Data Systems v. Intel Corp., 184 Cal. App. 4th 210 (Ct. App. 2010).

432 Vezi Robert W. Gomulkiewicz, *Entrepreneurial Open Source Software Hackers: MySQL and Its Dual Licensing*, Computer Law Review and Technology Journal, IX, 2004, p. 204; H. Ward Classen, *Fundamentals of software licensing*, IDEA: The Journal of Law and Technology, 1996.

433 Vezi www.gnu.org/philosophy/free-sw.html.

434 Vezi Lothar Determann, Stuart Pixley și Gary Shapiro, *Managing commercial risks in open source software licensing*, Journal of Intellectual Property Law & Practice, 2(11), 770-776, 2007; Open Source Initiative, opensource.org/docs/osd.

sunt în mod necesar de tip *open-source*[435]) sau de tip proprietar (*closed source*). Accesul la codul sursă permite înțelegerea tehnicilor și a metodologiei de programare (spre exemplu, de implementare a unor funcționalități), dezvoltarea de versiuni pentru alte platforme (extrem de dificilă sau chiar imposibilă fără acces la codul sursă) și reciclarea sa (modificarea, actualizarea sau folosirea sa, în totalitate sau în parte, în proiecte noi).

Codul sursă al unui program pentru calculator este protejat de instrumente juridice internaționale, regionale și naționale. Astfel, potrivit art. 10 alin. (1) din Acordul TRIPS, programele pentru calculator, fie că sunt exprimate în cod sursă, fie în cod obiect, vor fi protejate ca opere literare în temeiul Convenției de la Berna (1971). Directiva 2009/24/CE protejează implicit codul sursă, stipulând că protecția programelor pentru calculator se aplică oricărei forme de exprimare[436]. În România, protecția programelor pentru calculator include orice expresie a unui program, exprimate în orice fel de limbaj de programare, fie în cod sursă sau cod obiect (vezi Legea nr. 8/1996, modificată și completată prin Legea nr. 285/2004). Titularul dreptului de autor beneficiază de dreptul exclusiv de a reproduce permanent sau temporar, de a traduce, adaptare, aranja, transforma și distribui programul pentru calculator.

Pentru a fi protejat ca secret comercial, codul sursă trebuie să aibă o anumită valoare economică, să nu fie cunoscut public (să nu fie publicat) și să fie protejat prin măsuri rezonabile, ținând seama de circumstanțe, de păstrare a confidențialității[437]. De remarcat că anumite postări pe Internet nu duc la anularea protecției prin dreptul secretelor comerciale, după cum s-a decis într-un caz din august 2011[438].

Distribuirea unui program pentru calculator sub formă de cod obiect este motivată, în primul rând, de dorința de a păstra codul sursă secret, dar și de alte considerente, cum ar fi ușurința instalării acestuia pentru un utilizator obișnuit. Diseminarea publică a codului obiect nu poate fi considerată că divulgă secretele protejate în codul sursă[439]. Chiar dacă este scris într-un alt limbaj de programare, un cod sursă poate executa aceleași operațiuni și produce aceleași rezultate[440].

Cazurile de încălcare a secretelor comerciale în cazul codului obiect (codul executabil) sunt foarte rare deoarece acesta este, cel mai adesea, o versiune comercializată public (asemenea cazuri pot apărea doar în situațiile în care

---

[435] Vezi, spre exemplu, *Binary Code License Agreement* care guvernează mediul Java, care interzice decompilarea (*reverse engineering*) și nu furnizează acces la codul sursă.

[436] Vezi Directiva 2009/24/CE a Parlamentului European și a Consiliului din 23 aprilie 2009 privind protecția juridică a programelor pentru calculator.

[437] Vezi, spre exemplu, Decision Insights, Inc. v. Sentia Group, Inc et al., Case No. 09-2300, (4th Cir., March 15, 2011).

[438] Vezi cazul SyncSort Incorporated v. Innovative Routines, International, Inc., 2011 U.S. Dist. LEXIS 92321 (D.N.J. August 18, 2011). Vezi și cazul Silicon Image, Inc. v. Analogix Semiconductor, Inc., 2007 U.S. Dist. LEXIS 96073 (N.D. Cal. Jan. 17, 2008) și Ken Motolenich-Salas, *Trade secret misappropriation, possession of confidential information, and preliminary injunctions*, Journal of Intellectual Property Law & Practice, 3 (7), 440-441, 2008.

[439] Vezi Charles T. Graves și Brian D. Range, op. cit., p. 95.

[440] Vezi cazul Marketing Technology Solutions, Inc. v. Medizine LLC (S.D.N.Y. 5-18-2010).

BCU IASI CENTRAL UNIVERSITY LIBRARY

reclamantul foloseşte codul obiect ca un utilitar secret pentru funcţii interne sau care furnizează un avantaj competiţional). O entitate care foloseşte un program pentru calculator achiziţionat de la o altă entitate care a incorporat cod sursă fără autorizare şi care nu a avut posesia sau acces la respectivul cod sursă, ci doar la codul obiect, nu poate fi acuzată de încălcarea dreptului de autor sau a secretelor comerciale: acuzatul trebuie să aibă cunoştinţă de secretul comercial în cauză, programul pentru calculator în formă de cod obiect nu poate furniza, în mod normal, cunoaşterea secretelor comerciale implicate (vezi decizia şi analogia folosită în *Silvaco Data Systems v. Intel Corporation*: cineva care coace o plăcintă, după o anumită reţetă, o "foloseşte", în timp ce cineva care mănâncă plăcinta, prin actul de a mânca plăcinta, nu foloseşte reţeta)[441].

Obţinerea fără autorizare a codului sursă, respectiv exfiltrarea acestuia, se poate face prin copiere, duplicare, fotografiere, desenare, luarea de notiţe, imprimare, descărcare sau încărcare pe Internet (inclusiv prin poşta electronică), furtul unui suport fizic pe care acesta este stocat (spre exemplu, bandă magnetică, CD sau cheie USB) sau chiar prin memorizare (contaminanţii informatici putând fi folosiţi pentru obţinerea proprietăţii intelectuale[442]). "Fără autorizare" înseamnă lipsa permisiunii, consimţământului sau acordului deţinătorului de a obţine sau comunica codul sursă. Chiar dacă obţinerea fără drept a codului sursă, parţială sau în totalitate, nu duce la deposedarea proprietarului, această acţiune poate reduce sau chiar anula valoarea acestuia. Deţinătorul codului sursă nu trebuie să cunoască detaliile exacte privind modul în care codul sursă a fost obţinut pentru a iniţia a acţiuni în instanţă[443].

Obţinerea fără drept include şi achiziţionarea, primirea sau posesia de secrete comerciale obţinute fără autorizarea posesorului de drept[444]. Codul sursă scris în comun sau pe baza unui contract poate ridica probleme cum ar fi dreptul de autor şi refolosirea sa, mai ales în situaţiile de contract informal[445]. O licenţă implicită se consideră a fi acordată în situaţiile în care o parte solicită scrierea unui program pentru calculator, iar acesta este realizat şi furnizat beneficiarului[446]. Copierea de porţiuni mici a codului sursă nu poate fi o bază pentru încălcarea dreptului de autor

---

441 Silvaco Data Systems v. Intel Corp., 184 Cal. App. 4th 210 (Ct. App. 2010).

442 Vezi Symantec, *Recent Hydraq cyberattack - What you need to know*, 21 Jan 2010.

443 Vezi opinia exprimată în cazul Miller v. Facebook, Inc. (N.D.Cal. 7-23-2010).

444 De remarcat că dreptul privind proprietatea intelectuală în unele jurisdicţii nu permite acţiuni legale împotriva făptuitorilor în astfel de cazuri – vezi, în acest sens, Sonia Baldia, *Offshoring to India: Are Your Trade Secrets and Confidential Information Adequately Protected?*, Business & Technology Sourcing Review, Iss. 11, Q1/Q2 (2008).

445 Vezi T. Robert Rehm, Jr, *Navigating the open source minefield: What's a business to do?*, Wake Forest Intellectual Property Law Journal, Vol. 10, No. 3, 2009-2010, p. 293-294; T. J. McIntyre, *Copyright in custom code: Who owns commissioned software?*, Journal of Intellectual Property Law & Practice, 2(7), 473-486, 2007; Robert J. Orelup, *The enforceability of restrictive covenant provisions in employment agreements*, ABA Forum on the Construction Industry, 2008. Vezi şi cazul Justmed, Inc. v. Byce, 600 F.3d 1118 (9th Cir. 2010) pentru doctrina lucrărilor realizate sub contract (*works made for hire*).

446 Vezi, spre exemplu, cazul Asset Marketing Systems, Inc. v. Gagnon, 542 F. 3d 748 (9th Cir. Sep. 9, 2008).

(*de minimis non curat lex*)[447], dar aici trebuie remarcat că abordarea este calitativă și contextuală, în sensul că "porțiuni mici" pot fi esențiale (materiale) în cadrul codului sursă, caz în care se va considera că se încalcă dreptul de autor[448].

Decompilarea codului obiect, operațiune neagreată de mulți comentatori tehnici și legali, deoarece este considerată o metodă de obținere a secretelor comerciale[449], interzisă prin unele licențe, poate duce la obținerea unei aproximări a codului sursă, din care pot fi deduse detalii interne cum ar fi informațiile necesare realizării de programe interoperabile cu acel program[450]. Conform legislației române (art. 78 al Legii nr. 8/1996, modificată și completată prin Legea nr. 285/2004), autorizarea deținătorului dreptului de autor nu este obligatorie în situațiile în care reproducerea codului sau traducerea formei acestui cod este indispensabilă pentru obținerea informațiilor necesare realizării interoperabilității unui program pentru calculator cu alte programe pentru calculator, dacă actele de reproducere și de traducere sunt îndeplinite de o persoană care deține dreptul de utilizare a unei copii a programului pentru calculator sau de către o persoană care îndeplinește aceste acțiuni în numele celei dintâi, dacă informațiile necesare interoperabilității nu sunt ușor și rapid accesibile persoanelor îndreptățite și dacă aceste informații nu sunt utilizate pentru producerea ori comercializarea unui program pentru calculator a cărui expresie este fundamental similară, sau pentru orice alt act ce aduce atingere drepturilor titularului dreptului de autor.

Cazuri

United States v. Aleynikov[451]

Sergey Aleynikov a fost angajat al băncii Goldman Sachs pe poziția de Vice President al Diviziei Equities între mai 2007 și iunie 2009. În ultima zi ca angajat la Goldman Sachs, a copiat, compresat, criptat și transferat pe Internet, către un server din Germania, cu scopul de a dispune de acesta ulterior, sute de mii de linii de cod folosit pentru operațiuni bursiere cu frecvență înaltă[452] (*high-*

---

[447] Vezi Omar Johnny, Marc Miller, Mark Webbink, *Copyright in Open Source Software – Understanding the Boundaries*, International Free and Open Source Software Law Review, Vol. 2, Iss. 1, 2010.

[448] Vezi, spre exemplu, cazul Dun & Bradstreet Software Servs., Inc. v. Grace Consulting, Inc., 307 F.3d 197 (3rd Cir. 2002), în care apărarea a argumentat că doar 27 de linii de cod din 525000 sunt copiate. Vezi și cazul Marketing Technology Solutions, Inc. v. Medizine LLC (S.D.N.Y. 5-18-2010) (*smallness alone is not enough by itself to avoid liability*); Nancy J. Mertzel, *Copying 0.03 percent of software code base not 'de minimis'*, Journal of Intellectual Property Law & Practice, 3(9), 547-548, 2008: copierea a 54 de linii de cod într-o sursă de 160000 de linii nu a fost considerată copiere *de minimis* neacționabilă.

[449] Vezi Mid Michigan Computer Systems Inc v. Marc Glassman Inc., în care MGI a folosit programul stocat pe un calculator pentru a obține codul sursă prin decompilare (*reverse engineering*).

[450] Vezi Pamela Samuelson și Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, Yale Law Journal, Vol. 111, 2002.

[451] United States v. Aleynikov, 737 F. Supp. 2d 173 (S.D.N.Y. 2010).

[452] Acestea implică executarea rapidă a unui volum mare de tranzacții, deciziile fiind luate de programe pentru calculator foarte sofisticate, pe baza unor formule matematice (algoritmi) care

frequency securities trading), cu scopul de a dezvolta o platformă similară la firma Teza Techologies, LLC, unde obţinuse poziţia de "Executive Vice President, Platform Engineering". Goldman Sachs a achiziţionat porţiuni ale respectivului cod în anul 1999 pentru circa 500 milioane dolari, ulterior dezvoltând codul şi luând măsuri de protecţie a acestuia, inclusiv prin acorduri de confidenţialitate (codul, în totalitate sau părţi ale acestuia, nefind făcut public niciodată). A fost găsit vinovat de obţinerea ilegală a codului sursă şi condamnat pe data de 18 martie 2011 la 97 luni închisoare[453]. În February 2012, însă, printr-o decizie controversată, United States Court of Appeals for the Second Circuit l-a achitat[454].

United States v. Agrawal[455]

În noiembrie 2010, Samarath Agrawal, un fost trader al Société Générale, a fost găsit vinovat de obţinerea ilegală a codului sursă folosit în operaţiunile bursiere cu frecvenţă înaltă de bancă. Acesta a imprimat sute de pagini ale codului sursă cu scopul de a folosi programul la un competitor al băncii[456] şi a fost condamnat conform The Economic Espionage Act (EEA), 18 U.S.C. § 1832 şi The National Stolen Property Act (NSPA), 18 U.S.C. § 2314.

United States v. Zhang[457]

În noiembrie 2010, trei foşti angajaţi ai SiRF Technology, Inc. au fost acuzaţi de obţinerea ilegală a codului sursă aparţinând respectivei firme, cu scopul de a dezvolta şi comercializa aplicaţii GPS (*Global Positioning System*) pentru telefoane mobile, pierderile fiind evaluate la peste 60 milioane dolari[458].

ClearOne Communications, Inc., v. Bowers[459]

În acest caz, acuzaţii au obţinut ilegal şi folosit cod sursă aparţinând ClearOne pentru a crea produse pentru *audio conferencing*, care să concureze cu cele ale ClearOne. Decizia curţii a impus acuzaţilor să oprească divulgarea, folosirea sau transferul, în orice mod, a codului aparţinând ClearOne, inclusiv a algoritmilor şi sub-algoritmilor care nu sunt în domeniul public, sub orice formă şi a oricărui cod sau produs derivat substanţial din acest cod, precum şi divulgarea, folosirea sau transferul în orice mod a documentaţiei de dezvoltare a produsului şi

---

folosesc analize statistice ale tranzacţiilor anterioare şi dezvoltări curente ale pieţelor respective.

453 Vezi Statement of Jason M. Weinstein, Deputy Assistant Attorney General Criminal Division before the Committee on Judiciary United States Senate, *Oversight Of Intellectual Property Law Enforcement Efforts*, June 22, 2011.

454 United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012).

455 United States v. Agrawal, 10-cr-00417 (S.D.N.Y. 2011).

456 Vezi *2010 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement*, Feb 2011. Vezi şi cazul în care banca UBS AG a acuzat trei foşti angajaţi de obţinerea fără autorizarea a peste 25000 linii de cod sursă folosit în operaţiunile bursiere de bancă (www.securitiestechnologymonitor.com/news/-23668-1.html).

457 United States v. Zhang, No. CR10-00827 LHK (HRL) (N.D. Cal. Nov. 5, 2012).

458 Vezi *2010 U.S. Intellectual Property Enforcement*, op. cit.

459 ClearOne Communications, Inc. v. Bowers, 643 F.3d 735 (10th Cir. 2011).

orice documentaţie referitoare la acest cod şi a acordat daune în valoare de milioane de dolari[460].

ClearOne Communications, Inc. v. Biamp Systems[461]

Reclamantul din acest caz a achiziţionat cod sursă de la o terţă parte în anul 2000. În anul 2001, un angajat al ClearOne, cu acces la codul sursă, care a semnat un Acord de confidenţialitate şi non-competiţie neloială, a început să lucreze pentru firma Biamp. În urma plângerii depuse de ClearOne pentru obţinerea ilegală a unor secrete comerciale, conform Utah Uniform Trade Secret Act (UUTSA), juriul a acordat daune compensatorii de 956000 dolari pentru profituri nerealizate şi 694000 dolari pentru îmbogăţire fără justă cauză[462].

Oracle America, Inc. v. Google Inc.[463]

Google a copiat specificaţiile de design ale cel puţin 37 din cele 166 interfeţe de programare (*application programming interface*) în Java Development Kit Version 5 pentru librăriile Android (echivalentul a circa 11000 de pagini imprimate) şi cod sursă Java, protejat prin drept de autor (circa un miliard de calculatoare şi circa trei miliarde de telefoane mobile folosesc aplicaţii Java). Google susţine că programatorii firmei au creat programe informatice originale, care implementează funcţionalităţi Java fără a copia cod sursă, evitând, astfel, încălcarea drepturilor de autor. Juriul a considerat că Google nu a încălcat patente Oracle şi că structura API folosită de Google nu este protejabilă prin drept de autor. La apel, în mai 2014, decizia a fost în favoarea firmei Oracle privind protecţia prin drept de autor a structurii, secvenţei şi organizării API[464].

---

460 Vezi Ulrika E. Mattsson, *Broad Injunctive Relief and Damage Award for Misappropriation of Trade Secrets Upheld*, The National Law Review, 2011.

461 ClearOne Communications, Inc. v. Biamp Systems, 653 F.3d 1163 (10th Cir. 2011).

462 Vezi Gregory D. Yoder, *Defendant Not Allowed to Appeal Denial of a 12(b)(6) Motion to Dismiss After Trial*, The National Law Review, 2011.

463 Oracle America, Inc. v. Google Inc., 872 F. Supp. 2d 974 (N.D. Cal. 2012).

464 Oracle America, Inc. v. Google Inc., No. 10-CV-3561 (N.D. Cal. May 9, 2014).

BCU IASI/CENTRAL UNIVERSITY LIBRARY

4. INFRACȚIUNI INFORMATICE

4.1 Introducere

Tendința naturii umane de a cauza daune și a urma ceea ce dictează pasiunea, a fost larg recunoscută și discutată, de la Aristotel până la comentatori moderni[465], iar calculatoarele crează posibilități noi sau mărite în acest sens. Dezvoltările tehnologiilor informației și comunicației au dus la un tip de criminalitate ce nu a fost posibilă anterior (spre exemplu, diseminarea contaminanților informatici[466]); pe de altă parte, oferă oportunități crescute de comitere a unor infracțiuni tradiționale (spre exemplu, falsul)[467].

Cloud computing, dispozitivele mobile[468], adoptarea de programe de tip *open source* (care, cel puțin teoretic, prezintă o vulnerabilitate sporită), convergența serviciilor și rețelelor, folosirea rețelelor de socializare și numărul mare de erori potențiale (spre exemplu, erori de design, instalare sau întreținere a programe informatice[469]) cresc semnificativ vectorii potențiali pentru atacuri informatice. Adițional, numărul foarte mare de utilizatori[470] și calculatoare pe Internet (*hosts*)[471], comercializarea atacurilor informatice (oferirea ca produs comercial de contaminanți informatici, acces la *botnet*[472]-uri sau informații pentru

---

465 Vezi M. C. Bassiouni, *International Criminal Justice in the Age of Globalization*, International Conference on the occasion of the 30th Anniversary of ISISC, 77-156, 2004.

466 Google, spre exemplu, a anunțat că a descoperit peste 11.000 domenii pe Internet implicate în distribuirea de contaminanți informatici (*malware distribution*) – vezi în F. Paget, *Running Scared: Fake Security Software Rakes in Money Around the World* (2010); vezi și numărul de peste 3400 de site-uri web malițioase blocate zilnic, conform Symantec, *State of Security Survey*, 2011.

467 A se vedea S. W. Brenner, *Cybercrime: Criminal threats from cyberspace*, Praeger, 2010; S. Fafinski, W. H. Dutton și H. Margetts, *Mapping and Measuring Cybercrime*, 2010; F. Calderoni, *The European legal framework on cybercrime: Striving for an effective implementation*, Crime, Law and Social Change, 339–357, 2010; J. R. E. Bell, *The prosecution of computer crime*, Journal of Financial Crime, 9 (4), 308-325, 2002.

468 Conform International Telecommunication Union, *The world in 2010*, numărul global al abonamentelor la telefonia mobilă era de circa 5,3 miliarde.

469 Vezi B. Schneier, *The Problem Is Information Insecurity*, Security Watch, August 10, 2008; Web Application Security Consortium, *Web Application Security Statistics Project*, 2008.

470 Conform Internet World Stats, în 31 martie 2011 erau 2,095 miliarde utilizatori (44% în Asia, 22,7% în Europa, 13% în America de Nord); potrivit International Telecommunication Union, *The world in 2010*, numărul utilizatorilor Internet a depășit 2 miliarde; conform International Bank for Reconstruction and Development/The World Bank, *The Little Data Book on Information and Communication Technology*, 2011, există peste 1,8 miliarde utilizatori Internet.

471 În iulie 2014, existau peste un miliar de *hosts* pe Internet, conform Internet Systems Consortium, 2014.

472 Un număr de calculatoare controlate de un calculator central (*command-and-control*), pentru executarea de comenzi.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

realizarea atacurilor[473]) și asimetriile informaționale și, adesea, motivaționale măresc considerabil riscul atacurilor informatice și efectele lor potențiale[474].

Perioadele privind infracționalitatea informatică au fost împărțite de Hollinger în patru etape[475]:

- Perioada de descoperire a posibilității de comitere a infracțiunilor informatice (1946-1976);
- Criminalizarea infracțiunilor informatice (1977-1987);
- Demonizarea infractorilor informatici (1988-1992) și
- Perioada curentă (din 1993).

În literatura de specialitate, există diverse păreri cu privire la definirea infracțiunilor informatice, termeni precum "cyber-crime", "computer crime", "computer-related crime" sau "high-tech(nology) crime" sunt folosiți alternativ[476], fără o definiție precisă[477]. Mai mult, unii comentatori consideră aceste infracțiuni ca o nouă categorie, în timp ce alții le asimilează infracțiunilor obișnuite[478]. În general, infracțiunile informatice se referă la folosirea unui sau mai multor calculatoare pentru a facilita sau realiza comiterea unei infracțiuni și au fost impartite în următoarele categorii generale[479]:

- Infracțiuni în care calculatorul este o 'țintă' (calculatorul sau calculatoarele unei părți inocente sunt atacate, exemple incluzând vandalism sau sabotaj informatic, șantaj etc.);
- Infracțiuni în care calculatorul este o armă sau unealtă a infracțiunii (folosită pentru comiterea de infracțiuni 'tradiționale', cum ar fi falsul, încălcarea dreptului de proprietate intelectuală, înșelătorie, spălarea banilor etc.) și
- Infracțiuni în care calculatorul este incidental în comiterea unor infracțiuni (spre exemplu, pentru păstrarea evidențelor asupra infracțiunilor comise).

---

473 Vezi, spre exemplu, R. Anderson, R. Bohme, R. Clayton și Tyler Moore, *Security Economics and European Policy*, 2008.

474 Vezi o discuție detaliată a amenințărilor în Ioana Vasiu și Lucian Vasiu, *Criminalitatea în cyberspațiu*, op. cit.

475 Vezi R. Hollinger, *Crime, Deviance and the Computer*, Aldershot-Brookfield, 1997.

476 Vezi în F. Pocar, *New challenges for international rules against cyber-crime*, European Journal on Criminal Policy and Research 10, 27–37, 2004; vezi și S. W. Brenner, *Distributed security: A new model of law enforcement*, Journal of Internet Law, Nov, 2004.

477 Vezi și Comisia Comunităților Europene, *Către o politică generală de luptă împotriva criminalității cibernetice*, COM(2007) 267 final: în lipsa unei definiții comune a criminalității cibernetice, termenii "criminalitate cibernetică", "criminalitate informatică", „criminalitate în sfera informaticii" sau "criminalitate în înalta tehnologie" sunt adesea utilizați alternativ.

478 Vezi în E. J. Sinrod și W. P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 Santa Clara Computer & High Technology Law Journal 177, 188, 2000.

479 Vezi J. Audal, Q. Lu și P. Roman, *Computer Crimes*, The American Criminal Law Review, Spring, 2008, p. 233; M. D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 Harvard Journal of Law & Techonology 465, Summer, 1997.

BCU IASI CENTRAL UNIVERSITY LIBRARY

Lewis[480] consideră că există două categorii de infracţiunile informatice: cele în care un sistem informatic este vizat în vederea penetrării neautorizate, diseminării de contaminanţi informatici sau refuzului serviciului şi infracţiuni tradiţionale, cum ar fi frauda sau pornografia infantilă, care sunt facilitate de un calculator. Conform Glynn şi colab.[481], putem distinge 4 categorii de infracţiuni informatice: (1) furtul de bani, instrumente financiare, servicii sau date valoroase; (2) obţinerea neautorizată de servicii la un calculator; (3) folosirea ilegală de programe informatice şi (4) obţinerea neautorizată de date informatice.

Infracţiunile informatice au fost clasificate şi ca infracţiuni împotriva unui calculator (spre exemplu, accesul neautorizat), infraciuni în calculator spre exemplu, stocarea de materiale ilegale) şi infracţiuni via calculator (spre exemplu, anumite fraude realizate prin intermediul mesajelor de poştă electronică)[482]. Dificultatea clasificării infracţiunilor informatice este subliniată şi de Gordon şi Ford[483], care le văd ca pe un continuum, variind între infracţiuni aproape integral tehnice şi aproape integral legate de persoane (*people-related*, cum ar fi hărţuirea electronică, şantajul, manipularea preţului acţiunilor etc.).

Atacurile informatice pot viza numeroase obiective: beneficii financiare, intimidare, supraveghere, manipulare sau alterare a informaţiilor etc. Convenţia Europeană pentru prevenirea şi combaterea criminalităţii informatice distinge patru tipuri de infracţiuni informatice: Infracţiuni contra confidenţialităţii, integrităţii şi disponibilităţilor datelor şi sistemelor informatice; Infracţiuni informatice (*Computer-related offences*); Infracţiuni de conţinut; Infracţiuni împotriva dreptului de autor. Conform unui studiu realizat de United Nations Office on Drugs and Crime (UNODC)[484], infracţiunile informatice cuprind trei categorii majore: Acte împotriva confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice; Acte realizate cu ajutorul unui calculator pentru avantaje personale sau financiare sau pentru a cauza daune (*Computer-related acts for personal or financial gain or harm*); Acte realizate cu ajutorul unui calculator privind conţinutul (*Computer content-related acts*); şi o categorie numită "Alte infracţiuni informatice" (*Other cybercrime acts*), care include acte care pot fi, de asemenea, considerate infracţiuni informatice.

Infracţiunile informatice pot fi clasificate şi după obiectivul făptuitorului: infracţiuni de *Exploatare* (cazul *ameninţărilor persistente avansate*[485] sau

---

480 Citaţi în R. M. Kadir, *The Scope and the Nature of Computer Crimes Statutes - A Critical Comparative Study*, German Law Journal, Vol. 11 (06), 609-632, 2010.

481 Citaţi în R. M. Kadir, op. cit.

482 Vezi S. Fafinski, W. H. Dutton şi H. Margetts, *Mapping and Measuring Cybercrime*, 2010.

483 Vezi S. Gordon şi R. Ford, *On the definition and classification of cybercrime*, Journal of Computer Virology, 2, 13–20, 2006, la p. 15.

484 Vezi UNODC, *Comprehensive Study on Cybercrime* (Draft Feb. 2013), p. 16-21.

485 Acestea sunt definite ca fiind un adversar care posedă un nivel de expertiză sofistică şi resurse importante, care îi pot permite crearea de oportunităţi pentru realizarea obiectivelor prin vectori de atac multipli - vezi NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, 2011.

exfiltrarea de informaţii în scopul spionajului economic sau politic[486], încălcarea drepturilor de proprietate intelectuală etc.); *Interferenţă*, *Perturbare* (spre exemplu, atacurile de tip blocarea distribuită a serviciului, spam-urile generate prin botnet-uri[487] sau întreruperea mijloacelor de comunicare) sau *Distrugere* fizică[488]; şi *Conţinut ilegal* (spre exemplu, hărţuirea electronică sau pornografia infantilă). În secţiunile următoare, analizăm infracţiuni informatice selectate de legiuitor pentru **noul Cod penal**, intrat în vigoare în 1 februarie 2014.

4.2 Hărţuirea electronică

Art. 208. (2) Efectuarea de apeluri telefonice sau comunicări prin mijloace de transmitere la distanţă, care, prin frecvenţă sau conţinut, îi cauzează o temere unei persoane, se pedepseşte cu închisoare de la o lună la 3 luni sau cu amendă, dacă fapta nu constituie o infracţiune mai gravă.

Concept şi caracterizare

Infracţiunea de hărţuire electronică (*cyberstalking*) este încriminată ca o variantă normativă în art. 208, alin. 2 noul Cod penal (ca modalitatea normativă atenuată a *Hărţuirii*) şi face parte din grupa de **infracţiuni contra libertăţii persoanei.** Această infracţiune nu era prevăzută în vechiul Cod penal.

Infracţiunea de hărţuire electronică are în vedere anumite fapte prin care o persoană de rea-credinţă urmăreşte crearea unei stări de temere victimei prin utilizarea abuzivă a mijloacelor electronice de comunicare. Pe măsură ce numărul utilizatorilor de Internet creşte, devine din ce în ce mai mare şi prevalenţa cazurilor de *cyberstalking* (hărţuire prin sisteme informatice a adulţilor prin intermediul poştei electronice, *chat rooms*, *instant messaging*, contaminanţilor informatici etc.) şi *cyberbulling* (hărtuire prin sistemele informatice a minorilor).

Problematica hărţuirii electronice a primit o atenţie considerabilă în ultimii ani, atât în presa din lumea întreagă şi în discuţiile celor care realizează şi dezvoltă strategii normative, cât şi în publicaţii juridice[489], la aceasta contribuind şi unele

---

486 Vezi, spre exemplu, cazurile GhostNet şi Shadow Network: investigarea primului caz a relevat infectarea a 1295 de calculatoare în 103 ţări, circa 30% dintre acestea fiind considerate "high value", deoarece aparţineau unor instituţii guvernamentale (ambasade, ministere, comisii). Investigarea digitală a evidenţiat comunicaţii între calculatoarele infectate şi adrese IP ale unor servere situate în China şi exfiltrarea de documente senzitive – vezi ENISA, *Botnets: Detection, Measurement, Disinfection & Defence*, 2011.

487 Spre exemplu, reţeaua Conficker, de 7 milioane de calculatoare, sau *spam botnet*-ul Rustock, care putea trimite 30 miliarde de mesaje de poştă electronic pe zi - vezi Microsoft, *Battling the Rustock Threat*, 2011.

488 Vezi cazul Stuxnet, care a distrus fizic o ţintă militară, descris în R. Langner, *Stuxnet: Dissecting a Cyberwarfare Weapon*, IEEE Security & Privacy, May/June, 49–51, 2011; vezi şi Cisco, *2010 Annual Security Report*, 2011.

489 Vezi, spre exemplu, J. Huffman, A. Overton, *Missing the Mark: The Neglect of Stalking and Cyberstalking in Introductory Criminology Textbooks*, Journal of Criminal Justice Education, 24(2), 200-217, 2013; B.W. Reyns, B. Henson, B.S. Fisher, *Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending Among College Students*, Deviant

BCU IASI / CENTRAL UNIVERSITY LIBRARY

cazuri cu sfârşit tragic pentru victime. Fenomenul cyberstalking-ului este destul de greu de cuantificat; statistici precise care să arate care ar fi numărul anual de acte de hărţuire online nu sunt încă disponibile. Există, însă, estimări făcute de diverse organizaţii, care arată o creştere alarmantă de la 474.000 la aproape 19 milioane victime anual pe glob[490].

Astfel, conform National Center for Victims of Crime[491], 3,4 milioane de persoane peste 18 ani sunt hărţuiţi în fiecare an în SUA; 30% dintre victime sunt hărţuite de fostul sau actualul partener; numai 10% din victime sunt hărţuite de un străin. Persoanele între 18 şi 24 ani au înregistrat cele mai mari nivele de hărţuire; 11% dintre victime au fost hărţuite pe o perioada de 5 ani sau chiar mai mult; 46% dintre victime au înregistrat cel puţin un contact nedorit din partea hărţuitorului; una din 4 victime a raportat că a fost hărţuită prin una din formele de tehnologie, cum ar fi poşta electronică sau servicii de mesagerie;10% din victime au raportat că au fost monitorizate prin sistemele globale de pozitionare (GPS) şi 8% au raportat că au fost monitorizate prin intermediul camerelor video sau digitale sau sisteme de ascultare.

Alte statistici, realizate în SUA, au arătat că 90% dintre copii au fost victimele cyberbulling-ului, copii între 11 şi 13 ani fiind în cea mai mare măsură victime ale hărţuirii pe site-urile de socializare[492]. În UE, în cadrul unui proiect ale cărui rezultate au fost publicate în anul 2011, se arată că 6% dintre copiii cu vârste între 9 şi 16 ani au fost hărţuiţi online[493]. Hărţuirea este o infracţiune neutră, atât femeile[494] cât şi bărbaţii pot fi victime sau făptuitori, cu toate acestea, statisticile

---

Behavior, 33(1), 1-25, 2012; M. Salter şi C. Bryden, *I can see you: Harassment and stalking on the Internet*, Information & Communications Technology Law, Vol. 18, Iss. 2, July, 99-122, 2009; N. Harlin Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 Missouri Law Review 125, 2007; J. Petrocelli, *Cyber stalking*, Law & Order, 53(12), 56-58, 2005; R. D'Ovidio şi J. Doyle, *A study on cyberstalking: Understanding investigative hurdles*, FBI Law Enforcement Bulletin, 72(3), 10-17, 2003.

490 A se vedea statistici ale National Center for Victims of Crime referitoare la victimele cyberstalking-ului în USA la locaţia http://www.ncvc.org/src/main.aspx?dbID=DB_statistics195. În conformitate cu aceste statistici, 3,4 milioane de persoane peste 18 ani sunt hărţuiţi în fiecare an în SUA; 30% dintre victime sunt hărţuite de fostul sau actualul partener; numai 10% din victime sunt hărţuite de un străin. Persoanele între 18 şi 24 ani au înregistrat cele mai mari nivele de hărţuire; 11% dintre victime au fost hărţuite pe o perioada de 5 ani sau chiar mai mult; 46% dintre victime au înregistrat cel puţin un contact nedorit din partea hărţuitorului; una din 4 victime a raportat că a fost hărţuită prin una din formele de tehnologie, cum ar fi poşta electronică sau servicii de mesagerie;10% din victime au raportat că au fost monitorizate prin sistemele globale de pozitionare (GPS) şi 8% au raportat că au fost monitorizate prin intermediul camerelor video sau digitale sau sisteme de ascultare.

491 Vezi http://www.ncvc.org/src/main.aspx?dbID=DB_statistics195.

492 A se vedea http://cyber.laws.com/bullying-statistics.

493 A se vedea, *Risks and Safety on the Internet, The perspective of European children, Full findings and policy implications from the EU Kids Online survey of 9-16 years olds and their parents in 25 countries*, p. 6; interviurile au fost realizate în primavara/vara anului 2010, pe un eşantion de 25142 copii.

494 Vezi R. Purcell, M. Pathe şi P. E. Mullen, *A study of women who stalk*, The American Journal of Psychiatry, 158 (12), 2056-2061, 2001.

arată că un număr mai mare de femei sunt victime și un număr mai mare de bărbați sunt făptuitori[495].

Cyberstalking-ul și cyberbulling-ul pot fi considerate, în mod relativ, fenomene criminale noi, dar asta nu înseamnă că nu există legi specifice care să le pedepsească. În SUA, spre exemplu, aproape fiecare stat are legislație specifică pentru aceste infracțiuni, iar în UE, în ultimii ani, statele membre s-au grăbit să-și elaboreze legislație specifică în domeniu (unele dintre state, cum ar fi Regatul Unit, chiar să o modernizeze[496]). Organele implicate în prevenirea, descoperirea, investigarea și pedepsirea celor implicați în asemenea activități criminale, precum și responsabilii unor companii din domeniul tehnologiei informatice, au elaborat deja legi și practici pentru a contracara asemenea fapte[497].

Extinderea acestui tip de infracțiuni, a dus la crearea de departamente specializate în acest tip de incidente în metropole cum ar fi Los Angeles și New York, iar în UE strategiile în domeniu vizează același lucru (a se vedea noile strategii europene: strategia de luptă în domeniul criminalității informatice, în particular a Europol[498]; Comisia Europeană a propus în anul 2008 și un program pentru un Internet mai sigur, numit *Safer Internet*, destinat să asigure un grad sporit de siguranță pentru copiii care folosesc Internetul).

Dezvoltarea deosebită a rețelelor de socializare de tip Facebook a dus și la creșterea numărului și la sofisticarea infracțiunilor contra persoanei, de tipul hărțuirii prin sistemele informatice (*cybersytalking* și *cyberbulling*)[499]. Noile tendințe și evidențe arată că hărțuirea electronică devine o problemă din ce în ce mai serioasă în scop și intensitate, pe măsură ce indivizii utilizează Intenetul și celelalte mijloace de telecomunicații. Se prevede că fenomenul de cyberstalking va deveni mult mai comun decât cel al hărțurii în lumea fizică (*offline*), datorită numeroșilor stimuli pe care-i oferă Internetul: anonimitatea, lipsa dificultăților în a întâlni victima și șansele foarte reduse de a fi puși față în față cu victima și cu consecințele faptelor lor.

Deși hărțuirea online mai este încă percepută ca fiind mai puțin gravă decât cea offline, un studiu realizat încă din anul 2004 arată că respondenții o percep ca fiind extrem de păgubitoare[500]. Conform cercetătorilor de la Universitatea Bedford[501], hărțuirea electronică este mult mai frecventă și a devenit mai gravă decât

---

495 Vezi National Center for Victims of Crime, http://www.ncvc.org/src/main.aspx?dbID=DB_statistics195.

496 A se vedea M. Blake, *Government to launch inquiry into" outdated" cyberstalking laws*, The Independent, 18 iunie 2011.

497 Chiar și în Romania, reprezentanți ai industriei TIC au creat un site specializat la care se pot raporta activitățile de hărțuire electronică.

498 La întâlnirea ținută la sediul EUROPOL între 14-15 iunie 2010, s-a propus crearea European Union Cyber Crime Task Force: http://europol.easyred.com/?p=wzhwhazfi&paged=2.

499 Între cei doi termeni (*cybersytalking* și *cyberbulling*) nu se face nici o deosebire importantă în legislație, doar una semantică, primul termen fiind utilizat când este vorba de victime persoane adulte, al doilea termen în cazul victimelor copii.

500 A se vedea P. Bocij, *Cyberstalking: Harassment in the Internet Age and How to Protect your Family*, Westport, CT, Praeger, 2004, p. 15.

501 A se vedea, pentru amănunte, rezultatele *Cyber-Stalking Project*, lansat în septembrie 2010, http://www.beds.ac.uk/echo.

hărțuirea clasică (fizică). Deși există similitudini între cele două, pentru hărțuitorul online este mult mai ușor să-și atingă scopul, același cu cel al hărțurii clasice, el putând realiza activitatea criminală printr-o simplă apăsare de buton, de la distanță, utilizând echipamente și programe informatice sofisticate, care permit trimiterea repetată de mesaje, chiar fără a fi nevoie să fie fizic prezent lângă terminalul calculatorului, nemafiind nevoit să se deplaseze, să urmărească îndeaproape victima și să riște să fie văzut în preajma acesteia, când o urmărește fizic.

O strategie care să facă față fenomenului de hărțuire electronică trebuie să aibă la bază o cunoaștere a tipurilor de hărțuitori și a comportamentului acestora. O asfel de strategie ar trebui sa fie suficient de flexibilă încât să permita poliției, procurorilor, judecătorilor, celor care trebuie să ajute victima hărțuirii, precum și altor persoane implicate profesional în caz, să personalizeze intervenția în funcție de comportamentul specific al hărțuitorului, starea sa mentală și riscul pe care îl prezintă. Hărțutorii online au diferite motivații: răzbunare, ură, obsesii erotice etc.

Cercetătorii acestui fenomen au dezvoltat mai multe clasificări. Astfel, pentru Brenner[502], există patru categorii: hărțuitorul ex-partener, romanticul fantezist, obsesivul periculos și hărțuitorul sadic. Potrivit studiului realizat de L. McFarlane și P. Bocij[503], se pot identifica patru tipuri de hărțuitori online: tipul răzbunătorului, notat pentru ferocitatea atacurilor sale (folosind chiar troieni informatici pentru a acces ilegal și viruși informatici pentru infectarea deliberată a calculatorului victimei), tipul hărțuitorului al cărui scop este să enerveze, cel care încearcă să aiba o relație intimă cu victima, dar care se întorc împotriva ei în urma unei refuz, respectiv colectivitățile de hărțuitori formate în funcție de un anume scop.

Făptuitorii acționează din motive diverse, fac parte din orice categorie de vârstă, sex sau profesională, iar comportamentele lor cunosc o mare varietate de forme: hărțuirea de tip erotic-maniacă[504]; hărțuirea celebrităților; urmărirea obsesivă a unui coleg de muncă; hărțuirea din gelozie sau atacul asupra unui fost soț sau partener intim[505]; hărțuire sadică[506]; hărțuire realizată de grupuri anonime

---

502 A se vedea, S. Brenner, *Cybercrime: Criminal Threats from Cyberspace*, 2010, p. 128.

503 Vezi L. McFarlane și P. Bocij, *An exploration of predatory behaviour in cyberspace: Towards a typology of cyber stalkers*, First Monday, 8, 2005.

504 Într-un astfel de caz, o studentă, în vârsta de 42 de ani, a devenit obsedată de unul dintre profesori și a început să îi trimită zeci de e-mail-uri, încât acesta a trebuit să închidă acel cont. Profesorul a obținut în cele din urmă un ordin de restricție împotriva ei, dar ea l-a ignorat, fiind sanctionată pentru aceastai și a început să îi trimită zeci de e-mail-uri, încât acesta a trebuit să închidă acel cont. Profesorul a obținut în cele din urmă un ordin de restricție împotriva ei, dar ea l-a ignorat, fiind sanctionată pentru aceasta - vezi E. Jones, *Stalker who sent so many emails the account had to be closed*, Western Daily Press, august 10, 2007.

505 Cazul lui Joelle Ligon este un exemplu de ex-partener hărțuitor: un fost iubit a utilizat Internet pentru a o teroriza pe Ligon o perioadă de șase ani (a pretins a fi Ligon în *chat rooms*, unde a solicitat parteneri pentru sex și le-a dat numerele ei de telefon, a pretins, în mesaje e-mail, că diploma lui Ligon era falsă și că ar fi avut probleme în trecut cu devianța sexuală și drogurile, toate false) - vezi V. Ho, *Cyberstalker Enters Guilty Plea*, Seattle Post Intelligence, July 30, 2004.

506 Un caz cunoscut în această categorie este cel al lui Gary Delapenta, din Los Angeles, care a încercat să dezvolte o relație amoroasă cu o femeie de la biserică. În ianuarie 1999 a fost acuzat, potrivit prevederilor statului California în domeniul Cyberstalking, pentru postarea de mesaje care arătau că victima, o femeie de 28 de ani, are fantezii sexuale nesatisfăcute (în care

(*online mobs*)[507]; etc. Un hărţuitor electronic poate fi furios pe victima lui pentru o vătămare reală realizată de victimă sau percepută ca atare de făptuitor, iar ca urmare el urmăreşte victima cu trimiteri electronice (mesaje, telefoane, postări pe pagini de reţelele de socializare etc.). Alt tip de hărţuitor poate să fie îndrăgostit de victimă şi îşi face cunoscut sentimentul prin diverse trimiteri (*e-cards*, *e-flowers* şi alte cadouri).

Un studiu de dimensiuni semnificative, cuprinzând cazuri din SUA, pe care l-am realizat în 2013[508], arată că făptuitorii nu prezintă practic nici o restricţie în ceea ce priveşte vârsta, sexul, starea civilă, orientare sexuală şi origine etnică, culturală, economică sau intelectuală. Într-un caz, chiar o fetiţă în vârstă de 12 de ani a fost condamnată pentru comiterea acestei infracţiuni[509]. În unele cazuri, făptuitorii cunoşteau victima, în timp ce în numeroase alte cazuri, au găsit victima prin intermediul motoarelor de căutare, forumurilor on-line sau reţelelor sociale (cum ar fi MySpace, Facebook, Friendster, Twitter, etc).

Într-un număr de cazuri, infracţiunea a implicat foşti soţi (spre exemplu, *People v. Rosa*[510] şi *Unites States v. Walker*[511]). După ce relaţia romantică s-a încheiat, femeile se angajează în hărţuire electronică (spre exemplu, *Vrasic v. Leibel*[512]). În alte cazuri, făptuitorul căuta o relaţie romantică sau sexuală, victimele fiind, de multe ori, o celebritate, cum ar fi o actriţă (spre exemplu, *United States v. Gagnon*[513]) sau un model[514].

Victimele fenomenului sunt în majoritate femei, de vârste sau etnii diferite. Hărţuirea electronică are diferite motivaţii: cel mai adesea din răzbunare, ură sau satisfacerea unor obsesii erotice. Un număr de făptuitorii prezintă tulburari

---

apărea violată) pe grupuri de discuţii, în mesaje apărând numele, adresa şi numărul de telefon al victimei (în urma postărilor, şase bărbaţi au vizitat victima la domiciliu, care a primit şi câteva zeci de mesaje şi telefoane de la bărbaţi - vezi SANS Institute, *Cyber-stalking, Privacy Intrusion at It's Scariest*, 2001

507 Într-un caz de acest tip, din anul 2007, un grup de anonimi a ameninţat-o pe Kathy Sierra cu violul şi strangularea, i-au publicat adresa de acasă şi numărul Social Security şi au postat fotografii trucate ale acesteia. Înfricoşată, victima şi-a anulat angajamentele la diverse evenimente la care fusese invitată şi a închis blog-ul, scriind: "Nu mă voi mai simţi niciodată ca înainte de acest incident. Nu voi mai fi niciodată la fel". Furnizorii de servicii Internet sau deţinătorii unor site-uri web au fost blamaţi adesea că nu au luat atitudine împotriva acestui tip de hărţuire - vezi D. K. Citron, *Cyber Civil Rights*, Boston University Law Review, Vol. 89, 61-125, 2009.

508 Vezi Ioana Vasiu şi Lucian Vasiu, *Cyberstalking Nature and Response Recommendations*, Academic Journal of Interdisciplinary Studies, Vol. 2, No. 9, 229-234, 2013.

509 Vezi L. Myers, *Girl, 12, gets probation in cyber-stalking case*, 2011.

510 People v. Rosa, No. F063748 (Court of Appeals of California, Fifth District, 2013).

511 United States v. Walker, 665 F.3d 212 (2011).

512 Vrasic v. Leibel, 106 So. 3d 485 (Fla. Dist. Ct. App. 2013).

513 United States v. Gagnon, No. 08-8230 (4th Cir. Sept. 14, 2009).

514 K. Miles, LA Model, *Facebook Stalked By Man Threatening To Kill Her*, 2012; J. Schram, C. Amos, *SI model nails cyber-stalker accused of uploading her photos onto a porn site*, 2012.

bipolare (spre exemplu, *Unites States v. Juliano*[515] sau *Unites States v. Stacy*[516]) sau schizofrenie (spre exemplu, *Unites States v. Gagnon*[517]).

În ceea ce privește modul de comitere, am constatat folosirea frecventă a comunicațiilor electronice, crearea de site-uri web false sau postarea de anunțurile online fictive. Astfel, în *State v. Gandhi*[518], cursul de conduită a constat din e-mail-uri cu conținut sexual, amenințătoare, conținând detaliile derespre dorința sa de a avea relații sexuale cu victima. În *People v. Corleone*[519], autorul a creat o pagină web pe MySpace, portretizând victima ca fiind o prostituată, mama victimei fiind descrisă ca fiind un "proxenet".

În *United States v. Sayer*[520], autorul a creat un cont fictiv pe Facebook pentru o fostă prietenă și a postat reclame Internet fictive, care conțineau numele victimei, adresa ei și invitația de a fi vizitată pentru contacte sexuale. În *People v. Rosa*, faptuitorul a plasat pe un site web fotografii ale fostei sale soții în nud și anunțuri că victima este dornică să întâlnească bărbați pentru sex oral.

Victimele, chiar dacă cele mai multe sunt femei și copii, pot fi și ele de orice vârstă, sex sau pregătire profesională (nici măcar celebrul Mark Zuckerberg, boss-ul de la Facebook, nu a scăpat de această formă nouă de infracționalitate, fiind hărțuit de un individ numit Pradeep Manukonda[521]). Hărțuitorii își caută victime prin intermediul motoarelor de căutare, forumurilor online, chat-urilor și în cadrul rețelelor de socializare (MySpace, Facebook, Bebo, Friendster, Twitter etc.). Activitățile de hărțuire pot include *live chat*, comentarii pe site-uri web[522], trimiterea de mesaje nesolicitate (*spam*) sau contaminanți informatici (*malware*).

Hărțuitorii pot realiza activități de documentare online despre victime pentru a-și hrăni obsesiile și curiozitatea. Ulterior, actele de hartuire pot deveni mai intense, trimițând, spre exemplu, în mod repetat mesaje către victimă. Adesea, sunt postate mesaje defăimătoare despre victimă pe pagini web sau pe diverse alte platforme, în încercarea de a obține o reacție din partea victimei, pentru a iniția un contact (au existat și cazuri în care au fost create blog-uri false în numele victimei, cu conținut defăimator sau chiar pornografic).

Motivele și intențiile necunoscute ale hărțuitorului, precum și comportamentul obsesiv și impredictibil, expun victima unor riscuri majore

---

515 United States v. Juliano, No. 10-234 (W.D. Pa. Feb. 11, 2011).

516 United States v. Stacy, No. CR 11-1878 JB (D.N.M. May 3, 2013).

517 United States v. Gagnon, No. 08-8230 (4th Cir. Sept. 14, 2009).

518 State v. Gandhi, 989 A.2d 256 (2010).

519 People v. Corleone, D052816 (Court of Appeals of California, Fourth Appellate District, Division One, 2009).

520 United States v. Sayer, No. 2:11-CR-113-DBH (United States District Court, D. Maine, 2012).

521 A se vedea, în CNN Justice, 9 februarie 2011, Santa Clara County Superior Court of California a emis un ordin de restricție de 300 de zile împotriva lui Pradeep Manukonda pentru hărțuirea realizată împotriva șefului de la Facebook, Mark Zuckerberg. Făptuitorul a realizat atât acte de hartuire online (prin trimitere de mesaje amenințătoare pe Facebook), cât și acte de hărțuire în mediul fizic, fiind văzut atât în fața sediului central al Facebook, cât și în fața casei lui Mark Zuckerberg; de asemenea, acesta a încercat sa-i contacteze sora și iubita.

522 Vezi, spre exemplu, cazul comentariilor de pe AutoAdmit.com, descris în N. Kim, *Imposing Tort Liability on Websites for Cyber-Harassment*, 118 Yale Law Journal Pocket Part 115, 2008, http://thepocketpart.org/2008/12/15/kim.html.

precum şi unei traume psihologice[523]. Periculos la acest tip de infracţiune este faptul că, de multe ori, acest tip de atac evoluează către alte acte mai grave, urmărire fizică, violare de domiciliu, vandalism, loviri şi violente, chiar omor. Hărţuirea electronică este o problemă socială complexă. Principalul obiectiv al organelor de ordine este să elaboreze o strategie complexa anti-hărţuire care să facă posibilă intervenţia înainte ca victima să fie rănită sau omorâtă.

Strategii normative

Gravitatea hărţuirii ca infracţiune împotriva persoanei a fost resimţită cu mult timp în urmă şi legiuitorii naţionali au încercat să găsească de-a lungul timpului cea mai potrivită strategie normativă pentru a contracara pericolul prezentat de acest fenomen criminal. Se poate spune că istoria incriminării hărţuirii începe în SUA, cu un secol în urmă[524], când oamenii au realizat că telefoanele pot fi utilizate şi pentru alte scopuri decât cele legitime. Problema iniţială a venit de la personele care utilizau telefoanele pentru a transmite mesaje vulgare, obscene, profane sau indecente. Îngrijoraţi de faptul că acestea ar putea produce un prejudiciu, în special femeilor şi copiilor, statele au răspuns prin încriminarea acestora ca hărţuire. Iniţial, infracţiunea s-a focalizat pe apelurile cu conţinut obscen sau ameninţătoare, dar unele state au lărgit statutele pentru a cuprinde un comportament mai larg, cum ar fi apeluri anonime sau repetate care intenţionează să hărţuiască sau să enerveze.

Ca problemă specială a sistemului de justiţie penală, hărţuirea a căpătat o atenţie publică largă în anul 1989, când actriţa Rebecca Schaeffer a fost hărţuită şi ucisă de un fan obsedat. Şocaţi de această moarte şi altele similare, legiutorii din California au trecut prima lege în domeniul hărţuirii în anul 1990, de atunci toate statele americane au elaborat legislaţie anti-stalking. Multe dintre aceste strategii normative au avut ca punct de pornire raportul realizat în anul 1993 de National Institute of Justice (din cadrul U.S. Department of Justice), desemnat de Congresul SUA să elaboreze Model Anti-Stalking Code, care cuprinde, printre altele, principiile de bază ale elaborării unei asemenea legislaţii[525]. Prevederile din California, spre exemplu, aveau, la vremea respectivă, două elemente esenţiale: unul referitor la hărţuirea intenţionată şi repetată (hărţuirea a fost definită ca un comportament realizat pe o perioada de timp şi care arată continuitatea scopului) şi un element referitor la o ameninţare intenţionată, care să cauzeze victimei o rezonabilă frică de moarte sau de vătămare corporală gravă.

---

523 În conformitate cu statisticile ale National Center for Victims of Crimes (victimizarea în infracţiunile de hărţuire): 76% dintre victimele femei ucise de partenerul intim, au fost hărţuite de acesta înainte de a le omorâ; 67% au fost abuzate fizic de către partenerul intim, care le-a hărţuit înainte de aceasta; 89% dintre victimele femei ucise au fost au fost hărţuite de făptuitor cu un an înainte de a fi omorâte; 79% dintre femeile abuzate au raportat că au fost hărţuite în aceeaşi perioadă în care au fost abuzate fizic; 54% dintre femeile victime ucise au raportat activităţile de hărţuire poliţiei înainte de a fi ucise de hărţuitorul lor - a se vedea, National Center for Victims of Crime, http://www.ncvc.org/src/main.aspx?dbID=DB_statistics195.

524 A se vedea, S. Brenner, *Cybercrime: Criminal Threats from Cyberspace*, 2010, p. 92.

525 A se vedea, M. J. Russell, US Department of Justice, National Institute of Justice, *Project to develop a Model Anti-Stalking Code for States*, Research Report, 1993.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

Pe măsură ce societatea a devenit mai familiară cu hărţuirea, statele şi-au revizuit statutele. Incidente grave[526] au făcut unele state din SUA să adreseze în mod particular problema cyberstalking-ului şi cyberbulling-lui ca răspuns concret. Statutele moderne în domeniu cuprind comportamentul ameninţaător şi ceea ce poate cauza unei persoane raţionale un stres emoţional sever. În Michigan, "stresul emoţional" este definit ca fiind un stres sau o suferinţă de ordin mental care are nevoie de ajutor medical sau de altă natură.

Elemente preexistente

A. Obiectul juridic special constă în relaţiile sociale referitoare la libertatea persoanei, libertatea de a comunica şi utiliza mediile de comunicare electronice la adăpost de acţiunile maliţioase, şicanatorii ale anumitor persoane.

B. Obiectul material. Infracţiunea de hărţuire electronică nu are obiect material.

C. Subiecţii infracţiunii

a) **Subiect activ** poate fi orice persoană care are capacitate penală, indiferent de vârstă sau sex, indiferent dacă, între făptuitor şi victimă, existau relaţii de muncă sau similare.
Participaţia penală este posibilă sub toate formele.

b) **Subiect pasiv** poate fi orice persoană, indiferent de vârstă sau sex.

Structura şi conţinutul juridic al infracţiunii

1. Conţinutul constitutiv al infracţiunii

A) Latura obiectivă

Elementul material al laturii obiective se realizează prin acţiunea de hărţuire a unei persoane prin efectuarea de apeluri telefonice sau comunicări prin mijloace de transmitere la distanţă, care, prin frecvenţă sau conţinut, îi cauzează o temere unei persoane,

Legiuitorul prevede ca acţiunea de hărţuire electrronică să se realizeze repetat (a se vedea "prin frecvenţă") sau să aibă un "conţinut" care să ducă la producerea stării de temere.

Urmarea imediată constă în starea de pericol pentru libertatea persoanei.

Legătura de cauzalitate trebuie să existe între activitatea încriminată şi rezultatul socialmente periculos.

B) Latura subiectivă

Elementul subiectiv. Infracţiunea de hărţuire electrronică se comite cu intenţie directă sau indirectă.

---

[526] A se vedea, printre altele, cazul lui Megan Maier (http://cyber.laws.com/megan-meier-case), care s-a sinucis după ce a fost hartuită pe MySpace, cazul lui Tom Mullaney în vârsta de 15 ani, care s-a spânzurat în anul 2010 după cea fost atacat şi ameninţat la scoală prin intermediul Facebook; cazul lui Tayler Clementi, student la Rutgers University, New Jersey, SUA, care s-a sinucis după ce doi colegi au fost postate pe Internet materiale video cu el având relaţii homosexuale (http://cyber.laws.com/tyler-clementi-case).

BCU IASI CENTRAL UNIVERSITY LIBRARY

Forme, modalități, sancțiuni

A. Formele infracțiunii

a) **Actele pregătitoare.** Actele pregătitoare (procurarea sau realizarea de dispozitive vizând comiterea infracțiunii) pot face obiectul unei infracțiuni autonome, dacă sunt îndeplinite condițiile cerute de lege: infracțiunea incriminată în art. 365 din noul Cod penal și anume aceea de *operațiuni ilegale cu dispozitive sau programe informatice*.

b) **Tentativa** este posibilă (a se vedea la modalitatea în care se comite nu prin frecvență, adică prin repetare, ci prin conținut), dar nu se pedepsește.

c) **Consumarea** infracțiunilor are loc în momentul în care se realizează efectuarea de apeluri telefonice sau comunicări prin mijloace de transmitere la distanță, care, prin frecvență sau conținut, îi cauzează o temere unei persoane,

B. Modalități

Modalitățile normative. Infracțiunea de hărțuire electronică este una dintre modalitățile normative ale infracțiunii de hărțuire, mai precis modalitatea ei atenuată.

Modalitățile de fapt. Această *modalitate normativă* se pot prezenta într-o varietate de *modalități de fapt*.

C. Sancțiuni

Legea prevede pentru infracțiunea de hărțuire electrronică închisoarea de la o lună la 3 luni sau amendă.

Explicații complementare

Aspecte procesuale. Pentru infracțiunea de hărțuire electronică acțiunea penală se pune în mișcare la plângerea prealabilă a persoanei vătămate.

Elemente de drept comparat

În SUA, 18 U.S.C. § 2261A (2) incriminează folosirea de mijloace informatice cu intenția de a ucide, vătăma, hărțui sau plasa sub supraveghere cu intenția de a ucide, vătăma, hărțui sau cauza discomfort emoțional substanțial (*substantial emotional distress*) unei persoane din alt stat sau jurisdicție teritorială sau maritimă a SUA, care cauzează o stare de temere pentru viața sau integritatea sa corporală unei persoane, unui membru de familie sau partener intim al acelei persoane.

California a fost primul stat din SUA care a incriminat hărțuirea electronică, în Codul Penal (Secțiunea 646.9): "Orice persoană care în mod voit, cu răutate, și în mod repetat, urmărește sau voit și cu rea intenție hartuieste o altă persoană și care face o amenințare credibilă cu intenția de a plasa persoana în teamă rezonabilă pentru siguranța lui sau ei, sau siguranța familiei sale imediate este vinovat de infracțiunea de hărțuire" ("amenințare credibilă" este definit ca fiind "o amenințare verbală sau scrisă, inclusiv cea efectuată prin intermediul

BCU IASI CENTRAL UNIVERSITY LIBRARY

utilizarea unui dispozitiv de comunicare electronică"). Tot în California, a intrat vigoare, la 1 ianuarie 2009, o prevedere care permite școlilor să suspende sau să exmatriculeze elevii care îi hărțuiesc pe alții online. De asemenea, școlile sunt mandatate să dezvolte politici care adresează problema cyberbulling-ului[527].

În statul Florida (784.048), hărțuirea electronică (*cyberstalking*) este definită ca fiind angajarea într-un curs de conduită pentru a comunica, sau a face să fie comunicate, cuvinte sau imagini, prin utilizarea de mesaje de poștă electronică sau de comunicații electronice, îndreptate către o anumită persoană, provocând tensiune emoțională a acelei persoane și care nu servește nici unui scop legitim. Tot în Florida, în anul 2008, a intrat în vigoare "Jeffrey Johnston Stand Up For All Students Act" (1006.147), ca răspuns la sinuciderea adolescentului în vârstă de 15 ani Jeffrey Johnston, care a fost, o lungă perioadă, victimă a hărțuirii (*cyberbulling*)[528]. Această reglementare este unică printre legislațiile de acest tip, pentru că prevede blocarea fondurilor pentru școlile care nu respectă prevederilor în domeniu și nu îi informează despre acestea pe părinți și copii (făptuitori sau victime ale practicilor de cyberbulling).

Ca răspuns, la sinuciderea lui Phoebe Prince și a lui Carl Walker, hărțuiți înainte de a-și pune capăt vieții, în Massachusetts, în anul 2010, a intrat în vigoare una dintre cele mai aspre legi din SUA în domeniu. Prevederea interzice atât hărțuirea online, cât și cea fizică și mandatează școlile să realizeze activități de pregătire în universități și școli. De asemenea, mandatează școlile să realizeze activități de informare a părinților, dacă se realizează activități de hărțuire în școală[529].

În anul 2008, statul Missouri și-a revizuit legislația în domeniul hărțuirii, incluzând hărțuirea prin mijloace electronice și comunicații telefonice și cyberbulling-ul, după tragica sinucidere a adolescentei Megan Maier, hărțuită pe MySpace de mama unei colege, care și-a luat o identitate falsă[530]. În Texas, încă din anul 2001, a fost elaborat Stalking by Electronic Communications Act[531]. Statul Washington are o abordare care se focalizează pe prevenirea cyberbulling-ului și directionează activitățile principale către școli, care, potrivit prevederilor legale, au obligația de a elabora politici care să răspunda acestei provocări[532].

La nivelul legislației în domeniu a statelor membre ale UE, nu există o vedere unitară asupra definiției acestor infracțiuni[533]. În unele state, cum ar fi

---

527 A se vedea, pentru amănunte, http://www.usnews.com/education/blogs/on-education/2009/01/07 /california-law-targets-cyberbullying.

528 A se vedea http://abcnews.go.com/GMA/story?id=4774894&page=1.

529 A se vedea *Cyber Bullying Illegal: Mass. Governor Signs Landmark Anti-Bullying Law*, CBS News.

530 A se vedea, *Missouri Gov. Blunt Signs Bill Outlawing Cyberbullying*, http://www.cbsnews.com /8301-504083_162-20004060-504083.html.

531 A se vedea http://www.haltabuse.org/resources/laws/texas.shtml.

532 A se vedea, http://apps.leg.wa.gov/billinfo/summary.aspx?year=2007&bill=5288 și http://www.bullypolice.org/wa_law.html.

533 A se vedea, Modena Group on Stalking, *Protecting Women from the New Crime of Stalking. A Comparison of Legislative Approaches Within the European Union*, Final Report, University of Modena and Reggio Emilia for the European Commission, 2007, p.79.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

Germania şi Austria, se arată exact care sunt actele necesare pentru a fi în prezenţa acestei infracţiuni, în timp ce alte state preferă să folosească termeni generici pentru a o defini, fără să arate care anume acte ar putea constitui cyberstalking.

Nici în ceea ce priveşte numărul de acte necesare (având în vedere că hărţuirea electronică este văzută ca o activitate repetitivă, considerându-se ca fiind nevoie de mai mult de un act pentru a produce efectul dăunător asupra victimei) nu există consens. Spre exemplu, textul de lege din Franţa sau cel din Malta, nu cer o asemenea repetitivitate, fiind suficient şi un singur act de hărţuire pentru existenţa infracţiunii. Nu există similitudine nici în ceea ce priveşte regimul sancţionator: unele state au la dispoziţie numai pedeapsa cu închisoarea (Austria), altele au prevăzută şi posibilitatea unor amenzii, iar pedepsele cu închisoarea diferă în ceea ce priveşte maximul[534].

În Regatul Unit, în anul 2011, Justice Select Committee s-a întrunit pentru a discuta adaptarea legislaţiei în domeniul la noile dezvoltări ale tehnologiei informaţiilor şi comunicaţiilor (acest tip de hărţuitori fiind pedepsiţi conform prevederilor Protection from Harassment Act din anul 1997, mult anterior exploziei reţelelor de socializare, cu o perspectivă prea generală asupra hărţuirii). La sfârşitul anului 2012, a intrat în vigoare *the Protection of Freedom Act 2012*, care conţine prevederi privind hărţuirea electronică.

4.3 Violarea vieții private

Art. 226. (1) Atingerea adusă vieţii private, fără drept, prin:

a) ascultarea cu mijloace tehnice sau înregistrarea audio a unei persoane aflate într-o locuinţă, încăpere, dependinţă ori loc împrejmuit ţinând de acestea, sau a unei convorbiri private;

b) fotografierea, captarea sau înregistrarea de imagini, ascultarea cu mijloace tehnice sau înregistrarea audio a unei persoane aflate într-o locuinţă, încăpere, dependinţă ori loc împrejmuit ţinând de acestea, sau a unei convorbiri private se pedepseşte cu închisoare de la o lună la 6 luni sau cu amendă.

(2) Divulgarea, difuzarea, prezentarea sau transmiterea, fără drept, a sunetelor, convorbirilor ori a imaginilor prevăzute în alin. (1), către o altă persoană sau către public, se pedepseşte cu închisoare de la 3 luni la 2 ani sau cu amendă.

(3) Acţiunea penală se pune în mişcare la plângerea prealabilă a persoanei vătămate.

(4) Nu constituie infracţiune fapta săvârşită:

a) de către cel care a participat la întâlnirea cu persoana vătămată în cadrul căreia au fost surprinse sunetele, convorbirile sau imaginile, dacă justifică un interes legitim;

b) dacă persoana vătămată a acţionat explicit cu intenţia de a fi văzută ori auzită de făptuitor;

[534] A se vedea, Art. 107 Austrian Penal Code, Paragraf 238 German Penal Code, Art. 460 Belgian Penal Code, Section 264 Danish Penal Code, Protection from Harassment Act 1997 (UK), Art. 251a şi 251b Maltese Penal Code, Art. 285 Duch Penal Code.

BCU IASI CENTRAL UNIVERSITY LIBRARY

c) dacă făptuitorul, surprinde săvârşirea unei infracţiuni sau contribuie la dovedirea săvârşirii unei infracţiuni;
d) dacă surprinde fapte de interes public, care au semnificaţie pentru viaţa comunităţii şi a căror divulgare prezintă avantaje publice mai mari decât prejudiciul produs persoanei vătămate.

(5) Plasarea, fără drept, de mijloace tehnice de înregistrare audio sau video, în scopul săvârşirii faptelor prevăzute în alin. (1) şi (2), se pedepseşte cu de la 1 la 5 ani.

Concept şi caracterizare

În vechiul Cod penal, nu exista o asemenea incriminare. Noua incriminare, prevăzută în art. 226, întregeşte cadrul protecţiei penale a valorilor garantate în art. 8 din Convenţia europeană (*Cybercrime Convention*). Conceptul de "viaţă privată", pe care îl foloseşte textul este inspirat din conţinutul Tratatului de la Lisabona, intrat în vigoare la 1 decembrie 2009 şi anume din Carta Fundamentală a Drepturilor Omului. Una dintre caracteristicile de bază ale Cartei Fundamentale a Drepturilor Omului, a fost introducerea, în art. 8, a unui drept separat privitor la protecţia vieţii private şi a datelor personale. De observat că art. 16 al Tratatului de funcţionare a Uniunii Europene constituie, de asemenea, o bază legală generală pentru măsuri legislative cu privire la protecţia datelor personale[535].

Un al doilea element important la nivelul Uniunii Europene, care subliniază oportunitatea reglementării din noul Cod penal român, este accentul deosebit pus pe drepturile fundamentale ale cetăţenilor Uniunii Europene şi pe protecţia datelor lor personale de Comisia Europeană. Comisarul european responsabil pentru Justiţie, Drepturi fundamentale şi Cetăţenie, a făcut din protecţia datelor personale o prioritate. Program pe cinci ani al domeniului Justiţie şi Afaceri Interne, adoptat sub preşedinţia suedeză în decembrie 2009 (*Stockholm Programme*), punea un accent similar pe protecţia vieţii private şi a datelor personale. De asemenea, Parlamentul European în conformitate cu prevederile Tratatului de la Lisabona acordă o atenţie crescândă protecţiei vieţii private şi a datelor personale.

Reforma la nivel european în acest domeniu continuă şi conţine Propunerea de Regulament a Parlamentului European şi al Consiliului privind protecţia persoanelor cu privire la prelucrarea datelor personale şi libera circulaţie a acestor date [COM(2012) 11 final, din 25.01.2012] şi Propunerea de Directivă a Parlamentului European şi a Consiliului privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi la libera circulaţie a acestor date [COM(2012), 10 final, din 25.01.2012].

Necesitatea protecţiei vieţii private şi a datelor personale ca drept fundamental a fost recunoscută în Declaraţia Universală a Drepturilor Omului

---

[535] Tratatul de funcţionare a Uniunii Europene este unul dintre cele două elemente principale ale Tratatului de la Lisabona.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

(articolul 12)[536]; Pactul Internațional cu privire la Drepturile Civile și Politice (*International Covenant on Civil and Political Rights*) (articolul 17)[537]; Convenția pentru apărarea Drepturilor Omului și a Libertăților fundamentale (adoptată la Roma în 4 noiembrie 1950; amendată cu dispozițiile Protocolului nr. 14 (CETS No. 194) în vigoare de la data de 1 iunie 2010); Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convention No. 108, adoptată în anul 1981[538] de Consiliul Europei și intrată în vigoare la 1 octombrie 1985); Rezoluția de la Madrid (2009) și Rezoluția de la Ierusalim (2010)[539]. Importanța protecției datelor personale în prevenirea criminalității informatice este subliniată și de faptul că, în propunerea de Tratat Global în domeniul cybersecurității și cybercriminalității, se prevede, în art. 10, o nouă infracțiune, *Furtul de identitate*, realizat cu scopul de a obține un beneficiu economic pentru sine sau pentru altul, sau cauzarea unei pierderi de proprietate sau alt prejudiciu unei persoane[540].

Cadrul legal actual de protecție a vieții private și a datelor personale în EU a fost elaborat pe baza Convenției 108 a Consiliului Europei, realizată în paralel cu liniile directoare OECD privind intimitatea personală și fluxul de date personale transfrontalier (*Recommendation of the Council concerning Guidelines Governing the Protection af Privacy and Transborder Flows of Personal Data*, din 23 September 1980), care constituie cel mai relevant cadru legal global în domeniu. Convenția este un model pentru 41 de state din Europa și oferă protecția datelor personale pentru aproape 800 milioane de oameni. Acest Cadru legal în UE are următorii piloni de bază: Directiva 95/46/EC (Directiva generală), Directiva 2002/58/EC din 31 iulie 2002 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (*e-Privacy Directive*), Directiva 2009/136/CE și Decizia-cadru a Consiliului 2008/977/JHA în domeniul cooperării poliției și justiției în probleme penale. Cerința referitoare la "o autoritate de supraveghere independentă" implicată în această materie a fost clarificată de Curtea Europeană de Justiție[541]. O prevedere importantă în cadrul protecției datelor personale este și aceea ca statele europene să nu transfere astfel de date către state unde nu există un nivel adecvat de protecție a acestora.

Directiva 2009/136/CE[542] stabilește îndatoriri pentru controlorii de date privind procesarea datelor cu caracter personal, inclusiv obligația de a implementa

---

536 UN, *Universal Declaration of Human Rights*, 1948 [General Assembly resolution 217 A (III)].

537 UN, *International Covenant on Civil and Political Rights*, 1966 [General Assembly resolution 2200A (XXI)].

538 Vezi http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

539 A. Rihter, *Protection of privacy and personal data on the Internet and online media*, Raport al Committee on Culture, Science and Education, 2011.

540 S. Schjolberg și S. Ghernaouti-Helie, *A Global Treaty on Cybersecurity and Cybercrime*, Second edition, 2011. De remarcat că OECD a publicat o lucrare în anul 2008 în care propune incriminarea furtului de identitate (*online identity theft*). A se vedea și OECD, *Council's Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, 2007.

541 Judgment of 9 March 2010 in Case C-518/07.

542 Directivă a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la

măsuri tehnice şi organizatorice adecvate de protecţie a datelor. Cerinţele de informare în caz de încălcare a securităţii datelor prezente în Directiva 2002/58/CE prevăd o structură pentru anunţarea autorităţilor competente şi a indivizilor implicaţi în cazuri în care datele personale au fost compromise.

Persoanele a căror viaţă privată poate fi afectată (spre exemplu, prin furt de identitate sau fraudă legată de identitate, vătămarea corporală, umilinţa gravă sau compromiterea reputaţiei) sau ale căror date personale ar putea fi afectate negativ de incidente de securitate informatică, trebuie să primească o notificare fără întârziere pentru a putea lua măsuri de precauţie. Notificarea trebuie să includă informaţii privind măsurile luate de către furnizor pentru a soluţiona încălcarea securităţii, precum şi recomandări pentru persoana afectată.

Regulamentul (UE) Nr. 611/2013 al Comisiei din 24 iunie 2013 privind măsurile aplicabile notificării încălcărilor securităţii datelor cu caracter personal în temeiul Directivei 2002/58/CE a Parlamentului European şi a Consiliului privind confidenţialitatea şi comunicaţiile electronice, consolidează prevederile privind situaţiile de încălcare a securităţii datelor cu caracter personal. Astfel, conform Art. 3, notificarea abonatului, atunci când încălcarea securităţii datelor cu caracter personal ar putea afecta negativ datele cu caracter personal sau viaţa privată a unui abonat sau a unei persoane, prestatorul trebuie făcută cât mai repede posibil după detectarea încălcării securităţii datelor cu caracter personal.

Având în vedere multiplele dimensiuni ale vieţii private protejate prin cadrul legal de mai sus, legiuitorul român a incriminat fapta de violare a vieţii private prin fotografierea, captarea sau înregistrarea de imagini, ascultarea cu mijloace tehnice sau înregistrarea audio a unei persoane aflate într-o locuinţă, încăpere, dependinţă ori loc împrejmuit ţinând de acestea, sau a unei convorbiri private. Legiuitorul a considerat mai gravă divulgarea, difuzarea, prezentarea sau transmiterea, fără drept, a sunetelor, convorbirilor ori a imaginilor prevăzute în alin. (1), către o altă persoană sau către public, precum şi plasarea, fără drept, de mijloace tehnice de înregistrare video sau audio.

Elemente preexistente

A. Obiectul juridic al infracţiunii îl constituie relaţiile sociale a căror existenţă şi dezvoltare normală sunt condiţionate de respectarea vieţii private a persoanei. În acest context, având în vedere faptul că în Codul penal se foloseşte pentru prima dată conceptul de viaţă privată, se impun câteva explicaţii cu privire la dreptul la intimitate.

"Viaţa privată" este un concept larg, existând mai multe definiţii[543]. Dreptul la viaţă privată este definit în Gilbert[544] astfel: *Dreptul de a fi lăsat în pace, protejat de lege... dreptul la viaţă privată include confidenţialitatea comunicaţiilor*

reţelele şi serviciile de comunicaţii electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale şi protejarea confidenţialităţii în sectorul comunicaţiilor publice şi a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autorităţile naţionale însărcinate să asigure aplicarea legislaţiei în materie de protecţie a consumatorului.

[543] K. Gormly, *One Hundred Years of Privacy*, Wisconsin Law Review, 1335, 1992.

[544] Gilbert *Law Dictionary*, 1997, p. 257.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

și scrisorilor private, libertatea de a lua decizii personale (spre exemplu, privind căsătoria), dreptul de a se bucura de proprietatea privată și interesul împotriva falsei publicități.

Dreptul la viață privată este inerent dreptului la libertate[545] și noțiunilor de încredere și respect[546] și a fost identificat de unii filosofi ca un aspect cheie al demnității umane[547]. Warren și Brandeis[548] identifică dreptul la viață privată ca fiind *dreptul de a fi lăsat în pace, cel mai comprehensiv dintre drepturi și cel mai valorizat de omul civilizat* și consideră că *invadarea intimității trebuie prevenită*. Kang[549], pe de altă parte, consideră că termenul privat (*privacy*) transmite numeroase idei, care pot fi grupate după cum urmează:

- *Spațiul fizic*: protejarea teritoriului de solitudine al unui individ împotriva invadării de către obiecte sau semnale nedorite;
- *Selecție*: dreptul unui individ de a lua anumite decizii semnificative fără interferente; și
- *Fluxul informației personale*: privind controlul procesării informațiilor personale (obținere, divulgare sau folosire).

Clarke[550] elaborează termenul de viață privată și îi atribuie următoarele dimensiuni:

- Intimitatea corpului unui individ;
- Intimitatea comportamentului;
- Intimitatea comunicațiilor personale și
- Intimitatea informațiilor personale: individul trebuie să aibă dreptul să exercite un grad semnificativ de control asupra informațiilor personale și a modului în care acestea sunt folosite.

Solove[551] înțelege "viața privată" ca un concept pluralist[552] și propune o caracterizare ținând seama de următoarele dimensiuni:

- *Modul de colectare a informației*: Supraveghere (privit, ascultat sau înregistrarea activităților unui individ) și Interogare (diverse forme de chestionare sau de obținere a informației);
- *Modul în care informația este stocată, manipulată și folosită*: Agregare (combinare de informații diverse despre o persoană), Identificarea (legarea informației de o anumită persoană), Insecuritate (lipsa de grijă în protejarea informației stocate prin diseminare sau accesul neautorizat), Folosirea

545 J. B. Young, *Privacy*, Wiley, 1979.

546 C. Fried, *Privacy*, 77 Yale Law Journal, 477-478, 1968.

547 F. D. Schoeman (Ed.) *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, 1984.

548 S. Warren și L. Brandeis, *The Right to Privacy*, 4 Harvard Law Review 193, 1890.

549 J. Kang, *Information Privacy in Cyberspace Transactions*, 50 Stanford Law Review, 1193-1294, 1998.

550 R. Clarke, *Beyond the OECD Guidelines: Privacy Protection for the 21st Century*, 2000.

551 D. J. Solove, *A taxonomy of privacy*, University of Pennsylvania Law Review, Vol. 154, No. 3, January, 477-560, 2006.

552 D. J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, San Diego Law Review, Vol. 44, 745, 2007.

BCU CLUJ / CENTRAL UNIVERSITY LIBRARY

secundară (folosirea informației colectate pentru un scop în alte scopuri, fără consimțământul subiectului datelor), Excluderea (neinformarea subiectului datelor despre ceea ce se știe despre acesta și modul de manipulare și folosire);

• *Modul de diseminare a informației*: Încălcarea confidențialității, Divulgare, Expunere, Accesibilitate mărită, Șantaj, Însușire (folosirea datelor personale ale unui subiect) și Distorsionare (diseminarea de informații false despre indivizi);

• *Invadarea vieții private*: Intruziune (acte invazive care tulbură liniștea sau solitudinea unei persoane) și Interferență decizională.

B. Obiectul material al infracțiunii este reprezentat de entitatea materială, de suportul de hârtie, magnetic, or digital pe care se fixează, se înregistrează, se copiază datele filmate, ascultate, înregistrate (cu privire la aspecte ale vieții private a persoanei, acesta poate fi, spre exemplu, cheia USB, caseta video sau audio, CD-ul etc.).

C. Subiecții infracțiunii

a) **Subiectul activ** poate fi orice persoană, care îndeplinește condițiile generale ale răspunderii penale și care realizează oricare din activitățile încriminate.

Participația penală este posibilă sub toate formele.

b) **Subiect pasiv** poate fi orice persoană a cărei intimitate a fost lezată prin folosirea mijloacelor de interceptare de date, sunete, informații sau imagini.

Structura și conținutul juridic al infracțiunii

Conținutul constitutiv al infracțiunii cuprinde: a) latura obiectivă și b) latura subiectivă a infracțiunii.

a) **Latura obiectivă** cuprinde elementul material, cerințe esențiale, urmarea imediată și legătura de cauzalitate.

Elementul material poate consta din mai multe acțiuni alternative reprezentând acțiuni de interceptare de date, informații sau imagini din interiorul unei locuințe, încăperi, dependințe sau loc împrejmuit care ține de acestea, arătate în textul de lege, cum ar fi acțiunea de "fotografiere", "captare sau înregistrare de imagini", "ascultare" sau "înregistrare audio" (pentru forma simplă), "divulgare, difuzare, prezentare sau transmiterea sunetelor, convorbirilor sau imaginilor" către o altă persoană sau către public (pentru prima formă calificată) și "plasarea de mijloace tehnice de înregistrare audio sau video" (pentru a doua formă calificată).

Cerințe esențiale. Cerința esențială este ca toate aceste activități să se realizeze "fără drept", adică fără autorizarea, fără consimțământul persoanei a cărei viață privată este violată. Astfel nu săvârșește această infracțiune o persoană care fotografiază interiorul locuinței unei alte persoane cu consimțământul acesteia ori în baza unui mandat emis de instanță.

Cum capacitatea de supraveghere și colectare de date ale autorităților, ori a datelor din legislație în acest domeniu sunt foarte mari, este important și necesar să

se adopte măsuri pentru a preveni abuzul sau intruziunile fără mandat. În vederea respectării dreptului la viață privată și la corespondență, noul Cod de procedură penală instituie reguli procedurale în materia tehnicilor speciale de supraveghere și cercetare, care să satisfacă cerințele de accesibilitate, previzibilitate și proporționalitate. Sunt calificate și definite drept tehnici speciale de supraveghere sau cercetare, printre altele, interceptarea convorbirilor și comunicărilor; supravegherea video, audio sau prin fotografiere în spații private; localizarea sau urmărirea prin GPS[553] ori prin alte mijloace tehnice de supraveghere.

De observat că multe state europene au luat măsuri de protecție a vieții private a cetățenilor împotriva folosirii abuzive a acestor mijloace de investigare de către autorități. Spre exemplu, Germania a prevăzut la Secțiunea 201, alin (3) din Capitolul 15 "Violarea vieții private" (Codul penal german) o agravantă a faptei de nerespectare a intimității convorbirilor, când fapta este comisă de un funcționar public sau o persoană care a fost împuternicită cu exercitarea unei funcții de autoritate publică, care violează intimitatea convorbirilor, ori care înregistrează convorbiri ale altora, le utilizează sau le transmite altei persoane fără drept.

Asemenea prevederi sunt necesare, datorită posibilităților mari de a asculta telefoanele mobile. Poliția și organele judiciare au capacitatea de a urmări indivizii în timp real, utilizând fie dispozitive GPS sau telefoane mobile (mobile phone cell triangulation) ori să observe individul utilizând camere de supraveghere cu circuit închis (CCTV). În prezent, datorită posibilităților de a procura diverse dispozitive sofisticate, nu numai autoritățile și cei care lucrează în mass-media, dar și persoanele obișnuite au posibilitatea de a folosi microfonul sau telefonul mobil de la distanță pentru a înregistra conversațiile pe care o persoană le are cu alții, nu numai într-un loc public, ci și în locuința sau anexele care țin de aceasta sau în birou.

Chiar dacă făptuitorii mai utilizează aparatura tradițională, precum binoclul, pentru a supraveghea activitățile dintr-un domiciliu, datorită sofisticării fără precedent a mijloacelor tehnologiei informației și comunicației, mijloacele prin care se pot realiza activitățile de interceptare pot fi foarte variate, de la microfoane simple până la dispozitive extrem de greu de identificat de victimă, care se pot plasa în secret în camera în care se dorește ascultarea convorbirilor, fie în interiorul telefonului, fie pe linia telefonică, aparate de fotografiat cu obiective speciale sau camere de filmat ori programe informatice de ultimă oră, care fac din sistemele informatice afectate adevărați "spioni"[554]. Din cauza periculozității sporite a acestor fapte, legiuitorul român a prevăzut, ca formă calificată, în alin. (5), plasarea, fără drept, de mijloace tehnice de înregistrare audio sau video.

---

553 De remarcat, în acest context, decizia din anul 2011 a unei curți de apel din New Jersey, conform căreia folosirea de către soție a unui GPS pentru a urmări mișcările soțului nu constituie violarea dreptului la intimitate al acestuia [Villanova v. Innovative Investigations, Inc., et al., A-0654-10T2 (N.J. Ct. App. July 7, 2011)].

554 Spre exemplu, cazul troianului informatic care afectează telefoanele Android și care poate înregistra conversațiile utilizatorilor în SANS, *NewsBites*, Vol. XIII, Iss. 62, 2011; vezi și interceptarea de mesaje text, spre exemplu troianul informatic Spitmo, care poate infecta telefoane Google Android și intercepta mesaje text, în SANS, *NewsBites*, Vol. XIII, Iss. 74, 2011.

Au existat numeroase cazuri în care făptuitorii au instalat camere de filmat secrete în locuințele vecinilor, ori proprietari care au instalat camere secrete ca să spioneze chiriașii, înregistrându-le cele mai intime manifestări (camere audio sau video minuscule erau instalate în baie sau în dormitor, ascunse, de regulă, în dispozitivele de aerisire, în aparatele de aer condiționat sau în spatele oglinzilor); făptuitorii monitorizau de la distanță datorită tehnicii de ultimă oră toate imaginile și sunetele intime ale persoanelor aflate în domiciliul lor[555].

Programe informatice sofisticate permit controlul de la distanță asupra manifestărilor victimei în domiciliul ei, reușind să înregistreze sunete sau imagini ce țin de viața privată a acesteia. Astfel, dacă victima are un calculator conectat la rețea sau la un telefon cu Internet mobil, cu ajutorul unor programe informatice care permit "adulmecarea" parolelor (*password sniffers*) se monitorizează și se înregistrează numele de utilizator și parolele asociate în rețele. Pe această cale, agresorii pot accesa informații confidențiale ori altera informațiile sau lansa diferite programe sau comenzi care pot produce daune. Au existat cazuri în care victimele au uitat camera video a calculatorului deschisă și făptuitorul, datorită accesului de la distanță a putut prelua imagini intime ale victimei, care nu știa că este "privită" de la distanță.

Obținerea acestor imagini sau sunete înregistrate de făptuitor a devenit deosebit de facil de realizat datorită dezvoltării fără precedent a rețelelor de socializare gen Facebook sau platforma Google Video[556]. Mijloacele de interceptare sau mijloacele prin care se poate surprinde și controla o convorbire telefonică este și ea facilitată de apariția noilor generații de telefoane mobile.

Cauze de inexistență a infracțiunii. Legiuitorul a prevăzut câteva situații la alin.(4) care fac ca fapta să nu fie considerată infracțiune: în primul rând, este vorba de cazul în care activitățile de interceptare sau divulgare a imaginilor sau sunetelor aparțin celui care a participat la întâlnirea cu persoana vătămată în cadrul căreia au fost surprinse sunetele, convorbirile sau imaginile, dacă justifică un interes legitim. În al doilea rând, este vorba despre situația în care persoana vătămată a acționat explicit cu intenția de a fi văzută ori auzită de făptuitor.

O altă excepție privește situația în care făptuitorul surprinde săvârșirea unei infracțiuni sau contribuie la dovedirea săvârșirii unei infracțiuni. De asemenea, nu este considerată infracțiune fapta de interceptare sau divulgare dacă făptuitorul surprinde fapte de interes public, care au semnificație pentru viața comunității și a căror divulgare prezintă avantaje publice mai mari decât prejudiciul produs persoanei vătămate.

Unele acte materiale descrise în art. 226 sunt prevăzute de legiuitor ca circumstanțe agravante ale infracțiunii. Este vorba despre actele materiale descrise în art. 226 alin. (2) [divulgarea, difuzarea, prezentarea sau transmiterea fără drept, a sunetelor, convorbirilor ori a imaginilor prevăzute în alin. (1) către o altă

---

555 L.R. Mizell Jr, *Invasion of Privacy*, Berkeley Books, New York, 1998, p. 23 și urm.

556 Spre exemplu, cazul în care un judecător din Milano a condamnat trei directori Google pentru violarea intimității, neblocând un clip video care arăta patru tineri abuzând un coleg de clasă autist – vezi detalii în J. Israely, *Italy's Google Verdict Starts Debate on Web Freedom*, Time, Feb. 25, 2010.

persoană sau către public] precum şi actele materiale descrise în art. 226 alin. (5) [plasarea fără drept de mijloace tehnice de înregistrare audio sau video în scopul săvârşirii faptelor prevăzute în alin. (1) şi alin. (2)]. Conţinutul acestor agravante a fost explicat mai înainte.

A se vedea şi comentariul la art. 250 şi 251 al noului Cod penal în legătură cu violarea vieţii private prin fraudele comise prin mijloace de plată electronice.

Urmarea imediată constă în crearea unei stări de pericol pentru viaţa privată a unei persoane.

Legătura de cauzalitate. Între elementul material şi urmarea imediată trebuie să existe o legătură de cauzalitate. Aceasta rezultă, de regulă, chiar din săvârşirea faptei incriminate (*ex re*).

b) Latura subiectivă cuprinde elementul subiectiv şi cerinţe esenţiale. Sub aspectul elementului subiectiv, violarea vieţii private se realizează cu vinovăţie, sub forma intenţiei directe sau indirecte.

Forme. Modalităţi. Sancţiuni

A. Forme

a) **Actele de pregătire.** Actele pregătitoare, deşi posibile, nu sunt incriminate (acestea pot face obiectul infracţiunii din art. 365 noul Cod penal).
b) **Tentativa**, deşi posibilă, nu este incriminată.
c) **Consumarea infracţiunii.** Infracţiunea se consumă în momentul săvârşirii acţiunii incriminate şi al creării unei stări de pericol pentru viaţa privată a persoanei;
d) **Epuizarea.** Infracţiunea poate îmbrăca şi forma infracţiunii continue, în acest caz, *epuizarea* are loc în momentul în care făptuitorul realizează ultimul act al activităţii incriminate (spre exemplu, opreşte interceptarea imaginilor şi /sau sunetelor din domiciliul victimei).

B. Modalităţi

a) **Modalităţile normative simple.** Infracţiunea prezintă o singură variantă simplă [alin. (1)].
b) **Modalităţi agravate.** Infracţiunea se poate comite şi în *modalităţi agravate* prevăzute în alin. (2) şi alin. (5).
c) **Modalităţi de fapt.** Datorită specializării şi sofisticării mijloacelor tehnice şi a metodelor de înregistrare sau ascultare se pot întâlni diverse tipuri de realizare în practică a modalităţilor normative.

C. Sancţiuni

Forma simplă [art. 226 alin. (1)], se pedepseşte cu închisoarea de la o lună la 6 luni sau cu amendă; prima formă agravată [art. 226 alin. (2)] se pedepseşte cu închisoare de la 3 luni la 2 ani sau cu amendă. A doua formă agravată [art. 226 alin. (5)], se pedepseşte cu închisoare de la 1 la 5 ani.

Explicaţii complementare

Aspecte procesuale: Acţiunea penală se pune în mişcare la plângerea prealabilă a persoanei vătămate, pentru formele de la alin.(1) şi (2).

Elemente de drept comparat

Codul penal suedez, în Capitolul 4 *Crime împotriva păcii și libertății*, reglementează amplu faptele de violare a vieții private. Astfel, după ce în secțiunea 8 prevede violarea secretului corespondenței, în secțiunea 9a este incriminată *interceptarea neautorizată*, care constă în fapta persoanei care, în secret, ascultă sau înregistrează, prin mijloace tehnice, ceea ce se vorbește într-o cameră, o conversație între alte persoane sau o discuție la o conferință sau întâlnire în public la care nu a fost invitată, fiind prezentă în mod neautorizat. Pedeapsa este amenda sau închisoarea.

De asemenea, în această secțiune sunt pedepsite actele de pregătire în vederea violării secretului corespondenței sau interceptării neautorizate (secțiunea 9a). Astfel, o persoană care folosește mijloace tehnice cu intenția de a comite o violare a secretului corespondenței în modul arătat la secțiunea 8 sau o violare a vieții private din cele arătate la secțiunea 9, va fi pedepsită pentru acte pregătitoare la aceste infracțiuni cu amendă sau închisoare până la 2 ani.

O altă prevedere, care completează protecția prin mijloace penale a vieții private, se găsește în secțiunea 9c. Conform acestor prevederi, o persoană care, în alte cazuri decât cele definite la Secț. 8 și 9, fără drept, obține acces la o înregistrare de date informatice sau, fără drept, alterează, șterge sau introduce asemenea date într-un sistem informatic, va fi pedepsită pentru violarea secretului datelor cu amendă sau închisoare până la 2 ani.

Codul penal german. În Capitolul 15 intitulat *Violarea vieții private*, secțiunea 201 este incriminată *Violarea intimității convorbirilor*, apoi în secțiunea 201a este prevăzută *Violarea vieții private prin realizarea de fotografii*, iar în secțiunea 202 este prevăzută *Violarea secretului înscrisurilor*. Atacurile la viața privată sunt incriminate în secțiunea 202a *spionajul informatic* și la 202b

Codul penal italian cuprinde o prevedere referitoare la violarea vieții private a altei persoane în art. 615 bis, o formulare similară cu cea din Codul penal român în art. 226.

Legislația penală din **Marea Britanie**, cuprinde mai multe acte normative care reglementează acest domeniu și anume: un Cod de practici în domeniul reglementarii faptelor care aduc atingere vieții intime a persoane (elaborat în anul 2000 și revizuit în anul 2008), Legea privind protecția datelor (*Data Protection Act*) și *Regulation of Investigative Powers Act 2000* (pentru reglementarea atribuțiilor organelor de investigare). Codul de practici este cel care reglementează supravegherile video și audio, atingerile la viața privată aduse prin aceste metode și excepțiile. Prevederile acestuia sunt în deplină conformitate cu prevederile privind viața privată din Declarația universală a drepturilor omului și cu Legea privind protecția datelor (*Data Protection Act*).

Motivul apariției Codului de practici a fost numărul extrem de mare de camere video de supraveghere, nu numai în sectorul public, ci și în cel privat (utilizate de bănci, magazine, operatori de transport, dar și de cetățeni care le procură pentru a-și supraveghea casele și alte bunuri). Acest cod face chiar de la primele prevederi o distincție clară între utilizarea în scopuri domestice a acestor sisteme de supraveghere și cele utilizate pentru supravegherea publică.

Nu sunt considerate atingeri ale vieții private, în conformitate cu secțiunea 36 din Data Protection Act, datele procesate de o persoană pentru scop personal, al familiei sau pentru afaceri, aici incluzându-se și cele în scopuri recreative. Spre exemplu, dacă o persoana utilizează un sistem de supraveghere video cu circuit închis pentru a-și supraveghea casa de hoți, chiar dacă va înregistra și o parte de stradă și zonele de lângă casă, nu vor încălca principiile ocrotirii vieții private. De asemenea, dacă realizând fotografii în scopuri recreative, cu un telefon mobil, spre exemplu, nu se vor încălca principiile privind ocrotirea vieții private (înregistrările cu o cameră digitală video, realizate în aceleași scopuri, sunt, de asemenea, exceptate).

4.4 Fraude comise prin sisteme informatice și mijloace de plată electronice

4.4.1 Introducere

Concept și caracterizare

Infracțiunile prevăzute în acest capitol din noul Cod penal nu au corespondent în vechiul Cod. Aceste infracțiuni au fost prevăzute pentru prima dată în legile speciale și anume Legea nr. 161/2003 (în ce privește textul art. 249) și în Legea nr. 365/2002 (în ce privește art. 250 și 251). Cele 3 texte prevăzute în Capitolul IV al Titlului II incriminează diferite modalități de fraudă comise prin sisteme informatice și prin mijloace de plată electronice, fapte care au ajuns la o frecvență îngrijorătoare fiind susceptibile să provoace mari prejudicii sistemului financiar și unităților economice care folosesc această modalitate de plată.

Elemente preexistente

A. Obiectul juridic al acestor infracțiuni îl constituie relațiile sociale privitoare la siguranța și executarea cu bună-credință a tranzacțiilor financiare prin mijlocirea sistemelor informatice și a mijloacelor de plată electronice.

B. Obiectul material al acestor infracțiuni îl constituie fie entitatea materială pe care sunt stocate datele informatice sau componentele informatice, fie instrumental de plată utilizat în mod fraudulos.

C. Subiecții infracțiunii

a) **Subiectul activ** poate fi orice persoană fizică cu capacitate penală; aceștia sunt, de regulă, angajați sau funcționari ori persoane cu cunoștințe avansate în domeniul calculatorului, ori persoane juridice, sau orice persoană care realizează operațiunile financiare frauduloase incriminate, sau poate fi un subiect activ calificat și anume persoana care are atribuții de acceptare de operații financiare în mod curent în virtutea atribuțiilor de serviciu.

b) **Subiectul pasiv** este persoana fizică și juridică al cărei patrimoniu este afectat prin comiterea faptelor incriminate.

BCU IASI CENTRAL UNIVERSITY LIBRARY

Structura și conținutul juridic al infracțiunii cuprinde: **situația premisă** și **conținutul constitutiv** al infracțiunii.

A. Situația premisă

Aceste infracțiuni nu pot fi concepute și săvârșite fără existența unui sistem informatic, a unor date informatice, a unor mijloace de plată electronice susceptibile de a fi fraudulos utilizate sau a unor operațiuni financiare frauduloase.

B. Conținutul constitutiv cuprinde: a) latura obiectivă și b) latura subiectivă.

a) Latura obiectivă cuprinde: elementul material, cerințe esențiale, urmarea imediată și legătura de cauzalitate. Asupra fiecăreia din aceste componente ale laturii obiective se dau ample explicații cu ocazia analizei fiecărui text.

b) Latura subiectivă cuprinde: elementul subiectiv și cerințe esențiale. **Elementul subiectiv**, la toate infracțiunile din acest capitol este intenția directă sau eventuală.

Cerințele esențiale sunt specifice fiecăreia din infracțiunile analizate.

Celelalte elemente care intră în analiza acestor infracțiuni (forme, modalități, sancțiuni, explicații complementare, precedente legislative și situații tranzitorii, elemente de drept comparat), fiind specifice fiecărei infracțiuni, vor fi menționate și explicate cu prilejul analizei acestor infracțiuni.

4.4.2 Frauda informatică

Art. 249. Introducerea, modificarea sau ștergerea de date informatice, restricționarea accesului la aceste date ori împiedicarea în orice mod a funcționării unui sistem informatic, în scopul de a obține un beneficiu material pentru sine sau pentru altul, dacă s-a cauzat o pagubă unei persoane se pedepsește cu închisoare de la 2 la 7 ani.

Concept și caracterizare

Tehnologiile informației și comunicației oferă numeroase modalități de comitere a fraudei informatice; de asemenea, facilitează comiterea acestor infracțiuni prin posibilitatea de a acționa de la mare distanță sau prin abuzul autorizării acordate, prin costul redus al comiterii acestor infracțiuni și prin riscul relativ scăzut la care se expun făptuitorii. Conform unor studii[557], săvârșirea fraudei informatice are loc și sub forma delapidării de către făptuitorii, angajați cu supravegherea sau manipularea operațiunilor financiare sau contabile.

În vechiul Cod penal, această infracțiune nu exista, infracțiunea fiind reprodusă, fără modificări semnificative, din Legea nr. 161/2003 (se modifică doar pedeapsa, în sensul reducerii ei) care reproduce textul art. 8 din Convenția europeană privind criminalitatea informatică. Fenomenul fraudei informatice nu

---

[557] Vezi *2011 Data breach investigations report*, Studiu realizat de Verizon Risk Team cu cooperarea U.S. Secret Service și Dutch High Tech Crime Unit, p. 19., 2011.

BCU IASI CENTRAL UNIVERSITY LIBRARY

trezeşte reacţii mai negative decât în cazul altor infracţiuni, cu toate că pagubele patrimoniale aduse victimelor pot fi foarte mari.

Fraudele informatice se pot comite într-o varietate de moduri[558]: în cadrul operaţiei de *intrare* (*Input*)[559], atunci când datele informatice sunt inserate, accesate, suprimate sau modificate într-o manieră improprie sau neautorizată); ori în cadrul unui program informatic[560] atunci când are loc crearea sau alterarea ori substituirea unui sau mai multor programe informatice existente pentru realizarea fraudelor informatice, executarea programelor informatice abuziv sau cu parametrii improprii, masacrarea programelor informatice sau întreruperea unor procese, ce rezultă din nefinalizarea unor tranzacţii[561] (una dintre cele mai faimoase fraude informatice din această categorie este "frauda salam"[562]); sau *ieşire* (*Output*)[563], sub forma suprimării sau amendării datelor informatice reprezentând rezultatul unor procesări sau tranzacţii informatice.

Legea penală română incriminează, în art. 249 din noul Cod penal, frauda informatică ca fiind fapta de a cauza un prejudiciu patrimonial unei persoane prin introducerea, modificarea sau ştergerea de date informatice, prin restricţionarea accesului la date informatice sau prin împiedicarea în orice mod a funcţionarii unui sistem informatic, în scopul de a obţine un beneficiu material *pentru sine*[564] ori *pentru altul*[565].

---

558 United Nations, *Manual on the prevention and control of computer-related crimes*, International Review Of Criminal Policy, Nos. 43 şi 44, 1994; Lucian Vasiu şi Ioana Vasiu, *Dissecting Computer Fraud: From Definitional Issues to a Taxonomy*, Proceedings of the 37th Hawaii International Conference on System Sciences, Hawaii, USA, IEEE Computer, 2004.

559 Într-un astfel de caz, un contractant, în timp ce executa activităţile pentru care fusese angajat, a reuşit să acceseze sistemul informatic al organizaţiei şi să comită o fraudă de peste un milion dolari prin modificarea statutului de la "plătit" la "neplătit", transferarea sumele în contul său şi apoi refacerea statului tranzacţiilor cum erau iniţial – vezi în L. Vasiu şi I. Vasiu, *Dissecting Computer Fraud*, op. cit.

560 Într-un efort prin care încerca să acopere o serie de tranzacţii fictive introduse în sistemul informatic al unei bănci, un individ a manipulat sistemul care permitea urmărirea tranzacţiilor, ceea ce a dus la încasarea unui bonus de 650.000 dolari pentru sine, pentru tranzacţii bursiere care, în realitate, produseseră pierderi de milioane de dolari - vezi în L. Vasiu şi I. Vasiu, *Dissecting Computer Fraud*, op. cit.

561 L. Vasiu şi I. Vasiu, *A Taxonomy of Malware Use in the Perpetration of Computer-related Fraud*, în U.E. Gattiker (Ed.), EICAR 2004 Conference CD-ROM: Best Paper Proceedings, Copenhagen: EICAR e.V., 2004.

562 United Nations, *Manual on the prevention and control of computer-related crimes*, op. cit.

563 Într-un astfel de caz, o angajată a unei firme din California a emis cecuri pentru sine şi le-a încasat; pentru a evita depistarea, a modicat baza de date unde erau păstrate evidenţele cecurilor emise şi pentru cine au fost acestea emise.

564 Dacă nu există probe că o persoană a fost victima unei fraude (privind bani, bunuri tangibile sau intangibile, care au o valoarea economică), dacă acuzatul a acţionat dintr-o necesitate sau cu acordul victimei, dacă prejudiciul este cauzat de probleme tranzitorii (spre exemplu, fluctuaţii ale electricităţii) sau dacă victima ştia (era conştientă) că este prejudiciată nu putem vorbi de fraudă informatică.

565 F. Cohen, *Computer fraud scenarios: Robbing the rich to feed the poor*, Computer Fraud & Security, 1, p. 5-6, 2002.

Elemente preexistente

A. Obiectul juridic al acestei infracţiuni îl constituie relaţiile sociale de ordin patrimonial, precum şi întregul fascicol de relaţii referitoare la încrederea în siguranţa şi executarea cu bună-credinţă a tranzacţiilor informatice.

B. Obiectul material al infracţiunii îl constituie entitatea materială (disc compact sau dur etc.) pe care sunt stocate datele informatice sau componentele sistemului informatic asupra cărora se acţionează în sensul arătat în legea penală.

C. Subiecţii infracţiunii

a) **Subiectul activ** al acestei infracţiuni poate fi orice persoană fizică sau juridică; în practică, însă, manipulările constatate sunt comise, cel mai adesea, de angajaţi sau funcţionari[566] sau de persoane cu cunoştinţe avansate în domeniul calculatoarelor[567].

Participaţia penală este posibilă sub toate formele (complicitate, coautorat sau instigare).

b) **Subiectul pasiv** al infracţiunii este persoana fizică sau juridică (publică sau privată) al cărui patrimoniu a fost lezat prin comiterea fraudei informatice.

Structura şi conţinutul juridic al infracţiunii

Acesta este alcătuit din **situaţia premisă** şi **conţinutul constitutiv** al infracţiunii.

A. Situaţia premisă

Această infracţiune nu poate exista în absenţa unui "sistem informatic" şi a unor "date informatice" asupra cărora făptuitorul să acţioneze fraudulos în modalităţile prevăzute pentru realizarea scopului prevăzut în textul de lege.

B. Conţinutul constitutiv al infracţiunii cuprinde latura obiectivă şi latura subiectivă.

a) **Latura obiectivă** cuprinde: elementul material, cerinţe esenţiale, urmarea imediată şi legătura de cauzalitate.

Elementul material constă în acţiunea de introducere, modificare sau ştergere de date informatice, prin restricţionarea accesului la date informatice sau prin împiedicarea în orice mod a funcţionarii unui sistem informatic.

Introducere de date se referă la introducerea de date inexacte sau introducerea fără autorizaţie de date informatice[568].

Modificarea de date cuprinde alterarea, variaţiile sau schimbările parţiale de date informatice.

---

[566] Într-un astfel de caz, doi contabili şi-au depăşit autorizarea şi au emis ilegal acţiuni în valoare de 8 milioane dolari ale firmei la care lucrau, pentru ei – vezi detalii în L. Vasiu şi I. Vasiu, *Dissecting Computer Fraud*, op. cit.

[567] Într-un caz, un consultant financiar a transferat electronic suma de 8735692 dolari către companii unde avea interese, prin conectarea la sisteme informatice folosind contul altei persoane; pentru a masca acţiunile sale, a folosit contul unui alt angajat – vezi în L. Vasiu şi I. Vasiu, *Dissecting Computer Fraud*, op. cit.

[568] Într-un astfel de caz, un român a fost condamnat pentru accesarea ilegală a sistemului de comenzi online al firmei Ingram Micro şi plasarea a mai mult de 2000 de comenzi frauduloase, pe parcursul a 4 ani – vezi detalii la http://www.msnbc.msn.com/id/5614132/.

Ștergerea de date se referă la ștergerea datelor de pe suporturi fizice, care nu mai sunt disponibile pentru tranzacții electronice licite.

Restricționarea accesului cuprinde reținerea, ascunderea, criptarea sau modificarea autorizărilor pentru utilizatorii legitimi.

Împiedicarea funcționării unui sistem informatic cuprinde atacuri fizice (spre exemplu, tăierea de cabluri, întreruperea alimentării cu energie electrică etc.) și atacuri logice, care împiedică pornirea normală a unui calculator (spre exemplu, prin modificarea setărilor inițiale), atacuri de tip "refuz al serviciului" (*Denial of service*), blocarea sistemului prin folosirea de contaminanți informatici, blocarea tastaturii, consumarea resurselor de memorie sau a spațiului de stocare de pe discuri etc.[569]

Cerința esențială constă în aceea ca acțiunile să fie efectuate de făptuitor în scopul de a obține un beneficiu material pentru sine sau pentru altul; indiferent dacă acest scop a fost sau nu realizat.

Urmarea imediată constă în producerea unui rezultat, reprezentat de un prejudiciu material pentru partea vătămată. Nu contează valoarea acestui prejudiciu, este suficient să se dovedească faptul că patrimoniul persoanei vătămate a suferit o micșorare ca urmare a faptei comise de făptuitor.

Legătura de cauzalitate. Pentru realizarea laturii obiective a infracțiunii de fraudă informatică trebuie să se constate că există un raport de cauzalitate între acțiunea incriminată și urmarea imediată (prejudiciul material). Dacă situația păgubitoare este urmarea altei cauze (spre exemplu, unei căderi temporare de tensiune sau acțiunii unui contaminant informatic) și nu activității descrise de legiuitorul penal în art. 49, fapta nu va constitui urmarea imediată a acestei acțiuni, lipsind legătura de cauzalitate.

b) Latura subiectivă cuprinde: elementul subiectiv și cerințe esențiale.

Elementul subiectiv. Vinovăția la această infracțiune se prezintă sub forma intenției: *directă* (manevra frauduloasă directă) sau *indirectă* (manevra frauduloasă eventuală).

Cerințe esențiale. O cerință esențială și un element fundamental al fraudei informatice este acela al scopului în care se comite activitatea incriminată: acela de a obține un beneficiu pentru sine sau pentru altul.

Forme. Modalități. Sancțiuni

A. Forme

a) **Actele pregătitoare**, deși posibile și uneori necesare (de exemplu, crearea sau procurarea unui contaminant informatic pentru a accesa ilegal un sistem informatic), nu sunt incriminate și ca atare nici pedepsite în cazul acestui articol (pot constitui, însă, obiectul infracțiunii prevăzute în art. 46 al Legii nr. 161/2003 în sensul de operațiuni ilegale cu dispozitive sau programe informatice, infracțiune preluată și de noul Cod penal în art. 365).

b) **Tentativa** este posibilă și este pedepsită (conform art. 252 din noul Cod penal).

---

569 L. Vasiu și I. Vasiu, *A Taxonomy of Malware Use in the perpetration of Computer-related Fraud*, op. cit.

c) **Consumarea** infracţiunii are loc în momentul în care s-a produs urmarea imediată: prejudiciul material pentru partea vătămată.

d) **Epuizarea.** Infracţiunea se poate prezenta şi în forma continuată infracţiunii. Epuizarea are loc în momentul realizării ultimului act incriminat de legiuitor.

B. Modalităţi

Modalităţile normative sunt cele arătate în textul de incriminare şi pot consta în următoarele activităţi: *introducere de date*, *modificarea de date ştergerea de date, restricţionarea accesului* la date *împiedicarea funcţionarii unui sistem informatic*.

Toate aceste modalităţi normative se pot prezenta într-o varietate de modalităţi de fapt (a se vedea explicaţiile date la concept şi caracterizare).

C. Sancţiuni

Fapta de fraudă informatică este pedepsită în noul Cod penal cu închisoare de la 2 la 7 ani, o pedeapsă mai redusă decât cea prevăzută anterior de art. 49 din Legea nr. 161/2003, închisoarea de la 3 la 12 ani.

Explicaţii complementare

Aspecte procesuale: Acţiunea penală se pune în mişcare din oficiu. Competenţa de judecată în primă instanţă aparţine judecătoriei.

Elemente de drept comparat

Cum sursa acestei incriminări este art. 8 din Convenţia europeană privind criminalitatea informatică, marea majoritate a statelor europene au prevederi similare în acest domeniu. În SUA, 18 U.S.C. 1030(a)(4) defineşte "frauda informatică" ca fiind acces neautorizat, sau acces care depăşeşte autorizarea acordată, la un calculator protejat, cu intenţia de a frauda, obţinând subsecvent orice de valoare (*anything of value*), cu excepţia situaţiilor în care obiectul fraudei şi rezultatul acesteia constau doar în folosirea calculatorului şi valoarea unei astfel de folosiri nu depăşeste 5000 dolari într-o perioada de un an.

4.4.3 Efectuarea de operaţiuni financiare în mod fraudulos

Art. 250. (1) Efectuarea unei operaţiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, prin utilizarea, fără consimţământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia, se pedepseşte cu închisoarea de la 2 la 7 ani.

(2) Cu aceeaşi pedeapsă se sancţionează efectuarea uneia dintre operaţiunile prevăzute în alin. (1), prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

(3) Transmiterea neautorizată către altă persoană a oricăror date de identificare, în vederea efectuării uneia dintre operaţiunile prevăzute în alin. (1), se pedepseşte cu închisoarea de la unu la 5 ani.

Concept şi caracterizare

Efectuarea de operaţiuni financiare în mod fraudulos face parte dintre infracţiunile contra patrimoniului bazate pe fraudă. Infracţiunea constă din diferite acţiuni ilicite cum ar fi folosirea fără consimţământul titularului a unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia în vederea efectuării de transferuri de fonduri, altele decât cele ordonate şi executate de către instituţii financiare, retrageri de numerar, precum şi încărcarea şi descărcarea unui instrument de monedă electronică.

În vechiul Cod penal, această infracţiune nu exista, ea fiind preluată, fără modificări semnificative, din Legea nr. 365/2002 Legea comerţului electronic, (art. 27: *Efectuarea de operaţiuni financiare în mod fraudulos*). Această infracţiune, ca şi cea care urmează (Acceptarea operaţiunilor efectuate în mod fraudulos), se realizează numai prin mijloacele de plată electronice.

Elemente preexistente

A. Obiectul juridic al infracţiunii este reprezentat de relaţiile care se referă la securitatea instrumentelor de plată electronică, inviolabilitatea datelor conţinute de acestea, la care pot fi adăugate relaţiile sociale referitoare la încrederea publică în activitatea de comerţ electronic, precum şi relaţiile sociale referitoare la încrederea publică privind identitatea persoanelor.

B. Obiectul material este instrumentul de plată utilizat în mod fraudulos, (în cazul în care acest instrument este reprezentat de un suport material). Spre exemplu, obiect material al acestei infracţiuni poate fi reprezentat de un card de plastic, atunci când activitatea incriminată de legiuitor este realizată asupra acestuia.

C. Subiecţii infracţiunii

a) **Subiectul activ** poate să fie orice persoană care îndeplineşte condiţiile generale pentru a răspunde din punct de vedere penal, adică realizează operaţiunile arătate în textul de incriminare fără consimţământul titularului.

   Participaţia penală se poate realiza în toate formele (sub forma coautoratului, a instigării şi a complicităţii). Cum acest tip de infracţiune este destul de des comis în ultimul timp de grupuri de crimă organizată (fiind o activitate criminală extrem de profitabilă pentru aceste grupuri), în aceste cazuri va exista concurs între această infracţiune şi art. 367 C. pen.

b) **Subiectul pasiv** al infracţiunii este persoana fizică sau juridică (publică sau privată) al cărui patrimoniu a fost lezat prin efectuarea de operaţiuni financiare în mod fraudulos.

Structura şi conţinutul juridic al infracţiunii

Aceasta este alcătuită din **situaţie premisă** şi **conţinutul constitutiv** al infracţiunii.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

A. Situația premisă

Situația premisă la această infracțiune constă în existența unor mijloace de plată electronice, care sunt utilizate fraudulos pentru a efectua tranzacții electronice. Întrucât această infracțiune se realizează numai prin mijloacele de plată electronice, se impune să expunem pe scurt cadrul legal și instituțional al sistemului de plăți electronice.

În general, plățile servesc ca mijloc de schimb, mijloc de plată, standard de valoare sau unitate de cont. Caracteristicile sistemelor de plată derivă din organizarea socio-economică a societății în care acestea apar[570]. De-a lungul istoriei, dezvoltarea economică a depins de crearea de noi abstracții monetare[571], sistemele de plată electronic fiind ultima evoluție sau dezvoltare a acestora.

Progresele deosebite ale tehnologiei informației și comunicației, au revoluționat societatea și au schimbat radical relațiile bancă–client și chiar conceptul de bancă. Noile tehnologii au devenit atât un catalizator al marilor schimbări de care beneficiază consumatorii de servicii bancare, cât și un mijloc de răspuns al băncilor în fața noilor cerințe[572]. În consecință, la nivel regional și global s-au făcut eforturi pentru crearea și dezvoltarea unui sistem complet și complex de plăți electronice[573]. Folosirea instrumentelor de plată electronică este din ce în ce mai răspândită, în SUA, spre exemplu, numărul plăților non-cash a totalizat 109 miliarde în anul 2009, depășind cu 75% plățile *cash*[574].

Conform Deciziei-cadru 2001/413/JHA privind combaterea fraudei și contrafacerea unor sisteme de plată altele decât numerarul, prin "instrument de plată" se înțelege un instrument corporal, altul decât moneda legală (bancnote sau monede) care, în funcție de natura lui specifică, singur sau împreună cu alt instrument (de plată), îi dă posibilitatea deținătorului sau utilizatorului să transfere bani sau o valoare bănească, ca de exemplu cărți de credit, carduri de tip eurocec, alte carduri emise de instituții financiare, cecuri de călătorie, eurocecuri, alte cecuri și cambii care sunt protejate împotriva imitației sau uzului fraudulos, de exemplu prin intermediul modelului, codului sau semnăturii.

Prin „instrument de plată electronică" se înțelege, în general, un instrument care permite titularului să efectueze retrageri de numerar, încărcarea și descărcarea unui instrument de monedă electronică, precum și transferul de fonduri, altele decât cele ordonate și executate de către instituții financiare. Înțelesul expresiei "instrument de plată electronică" este explicat pe scurt în dispoziția din art. 180 din

---

570 W.E. Baker și J.B. Jimerson, *The Sociology of Money*, The American Behavioral, Sage Publications, Jul/Aug, 678-693, 1992; B. Maurer, *The Anthropology of Money*, Annual Review of Anthropology, 2006.

571 J.B. Konvisser, *Coins, notes, and bits: The case for legal tender on the Internet*, Harvard Journal of Law & Technology, Vol. 10, No. 2, Winter, 1997.

572 J.-M. Sahut, *Internet Payment and Banks*, 2011.

573 M. Kaur, R. Nyangosi și J. S. Arora, *Empirical study of mapping adaptation antecedents of electronic money*, International Journal of Electronic Finance, Vol. 5 Issue 1, January, 2011; Nomura Research Institute, *Electronic money trends as revealed by a consumer survey*, 2009; European Central Bank, *E-payments in Europe – The Eurosystem's perspective*, 2002.

574 Federal Reserve System, *The 2010 Federal Reserve Payments Study*, 2011; vezi și L. Ali Khan, *A Theoretical Analysis of Payment Systems*, South Carolina Law Review, Vol. 60, 2008.

noul Cod penal. Ca instituţie, plăţile electronice îşi găsesc reglementarea în dreptul afacerilor electronice (cu predilecţie, în secţiunea consacrată comerţului electronic). Prin urmare, în mod firesc, în explicarea expresiei "instrument de plată electronică", noul Cod penal trebuia să ţină seama de dispoziţiile referitoare la definiţia dată acestui tip de instrument în *Legea privind comerţul electronic* (Legea nr. 365/2002) în art. 1, precum şi de dispoziţiile BNR în domeniu, dispoziţii care nu fac decât să preia cadrul legislativ comunitar în materie.

Având în vedere faptul că art. 180 a fost conceput spre a servi la corecta înţelegere a dispoziţiilor legale din art. 250 C. pen. (Efectuarea de operaţiuni financiare în mod fraudulos) şi art. 251 C. pen. (Acceptarea operaţiunilor financiare efectuate în mod fraudulos), articole din noul capitol IV „Fraude comise prin sisteme informatice şi mijloace de plată electronice", Titlul II „Infracţiuni contra patrimoniului", este utilă şi necesară o definire a fiecărui concept cheie utilizat de legiuitor, nu doar o definiţie cu caracter general, cum este cea pe care a preferat-o legiuitorul nostru penal în acest articol.

Apariţia serviciilor de plată electronică prin Internet sau telefonul mobil [*m-payments*, transferul de fonduri între două entităţi folosind un telefon mobil la punctul de vânzare (*proximity*) sau de la distanţă (*remote*)] este un răspuns firesc la schimbările fundamentale înregistrate la nivel socio-economic în ultimii ani[575]. Conform COM(2011) 941 final, Carte Verde către o piaţă europeană integrată a plăţilor efectuate cu cardul, pe internet şi de pe telefonul mobil, plăţile electronice sunt plăţile efectuate prin intermediul internetului, de obicei în unul dintre următoarele trei moduri:

1) Efectuarea unei operaţiuni de plată cu cardul la distanţă prin internet;
2) Operaţiuni de transfer credit sau debitare directă prin online banking, în cadrul cărora plătitorul utilizează un portal online pentru autentificare (în prezent acestea funcţionează numai la nivel naţional);
3) Plăţi prin intermediul furnizorilor de plăţi electronice, unde consumatorii îşi creează conturi individuale. Conturile pot fi alimentate prin metode „tradiţionale" de plată, de exemplu transferuri bancare sau plăţi cu card de credit.

Plăţile de pe telefonul mobil, pe de altă parte, pot fi clasificate în două categorii principale:

1) Plăţile la distanţă au loc în principal prin internet/WAP9 sau prin servicii premium SMS care sunt facturate la plătitor prin intermediul operatorului reţelei mobile. Cele mai multe dintre plăţile la distanţă efectuate prin internet se bazează în prezent pe sistemele de plată cu cardul. Alte soluţii, bazate pe operaţiuni de transfer credit sau debitare directă, sunt fezabile din punct de vedere tehnic şi pot fi la fel de sigure, eficiente şi competitive, însă întâmpină dificultăţi la intrarea pe piaţă.

2) Plăţile de proximitate se desfăşoară, în general, direct la punctul de vânzare. Acest tip de plăţi utilizează Near Field Communication (NFC), cea mai performantă tehnologie de proximitate disponibilă la ora actuală, şi necesită

---

[575] B. Geva şi M. Kianieff, *Reimagining E-Money: Its Conceptual Unity with other Retail Payment Systems*, 2002.

telefoane special echipate[576], care să poată fi recunoscute de dispozitivele de citire la punctul de vânzare (spre exemplu, în magazine, în mijloacele de transport în comun sau în parcări).

Complexitatea tranzacţiilor electronice a dus la apariţia a numeroase sisteme de plăţi electronice, în general clasificate în următoarele categorii generice: *Sisteme de plăţi cu carduri de credit sau debit*, *Sisteme de cecuri electronice* şi *Sisteme de cash electronic*. Introducerea noilor instrumenteşi sisteme de plăţi electronice prezintă numeroase beneficii, dar şi oportunităţi infracţionale semnificative[577].

Sisteme de plăţi cu carduri

Conform COM(2011) 941 final, cardurile sunt "cele mai des întâlnite şi folosite instrumente de plată electronică pentru plăţile de retail". Un card are forma şi dimensiunile specificate de standardul ISO/IEC 7810 ca ID-1 (85.60 × 53.98 mm). Cardurile pot fi de tip *Open Loop*, emise de asociaţii globale şi pot fi folosite la orice comerciant, sau de tip *Closed Loop*, care pot fi folosite doar la comerciantul emitent. Se pot identifica cel puţin următoarele tipuri de carduri:

- *Card de debit*: cardul prin intermediul căruia utilizatorul dispune doar de disponibilităţile băneşti proprii, existente într-un cont deschis la emitent pentru efectuarea operaţiunilor prevăzute la pct. 1 din Regulamentul BNR nr. 6/2006;
- *Cardul de debit cu facilitate de descoperit de cont*: cardul prin intermediul căruia utilizatorul poate dispune, pentru efectuarea operaţiunilor prevăzute la pct. 1 din Regulamentul BNR nr. 6/2006, pe lângă disponibilităţile băneşti proprii existente într-un cont deschis la emitent, de o anumită sumă, în limita unui plafon predeterminat;
- *Cardul de credit*: cardul prin intermediul căruia utilizatorul dispune de disponibilităţi băneşti ale emitentului, oferite sub forma unei linii de credit, care îi permit utilizatorului efectuarea operaţiunilor prevăzute la pct. 1 din Regulamentul BNR nr. 6/2006, în limita plafonului stabilit în prealabil;
- *Cardul de numerar*: cardul utilizabil doar la automate bancare pentru retragere de numerar.

Un "sistem de carduri" este un aranjament tehnic şi comercial înfiinţat pentru a servi unul sau mai multe brand-uri de carduri care oferă reţeaua organizatorică, juridică şi operaţională necesară funcţionării serviciilor comercializate de brand-ul respectiv[578]. În cadrul sistemului de plată prin carduri, se disting două tipuri: sistemul *tripartit* (spre exemplu, American Express; în acest sistem, funcţiile de emitere şi

---

576 Vezi, spre exemplu, *Apple Pay*, https://www.apple.com/iphone-6/apple-pay/.

577 J. Crossley, *Credit card fraud*, Credit Management, 05, 2009, p. 26; K. J. Barker, J. D'Amato şi P. Sheridon, *Credit card fraud: Awareness and prevention*, Journal of Financial Crime, Vol. 15, Iss. 4, 398–410, 2008; B. Zalud, *Credit Card & Transaction Fraud Schemes*, Security, Vol. 45, Iss. 6, 2008, p. 94.

578 Vezi Marinela Teodorescu (Raportor), *Raport privind piaţa serviciilor de plăţi prin carduri*, 2013, p. 17.

achiziție sunt integrate într-o singură instituție financiară) și sistemul *cvadripartit* (spre exemplu, Visa; acest tip de sistem implică patru entități principale: banca emitentă a cardului, banca achizitoare, deținătorul cardului și comerciantul)[579].

O tranzacție tipică de plată prin card implică un mesaj de autorizare transmis de la comerciantul unde este folosit cardul de plată către instituția financiară care furnizează serviciul către respectivul comerciant. Mesajul este transmis către banca emițătoare a respectivului card, care autentifică informația transmisă prin mesaj și tranzacția este autorizată sau refuzată (în situațiile în care informația furnizată nu este corectă, contul este blocat[580], tranzacția este considerată frauduloasă sau deținătorul cardului nu are suficienți bani pentru respectiva tranzacție)[581].

Industria plăților electronice este dominată de folosirea cardurilor de credit[582], care se estimează că reprezintă circa o treime din volumul total al cumpărăturilor în anul 2010[583]. Cardurile de debit reprezintă, de asemenea, un număr foarte important, atât în ceea ce privește numărul lor[584], cât și volumul cumpărăturilor și numărul de tranzacții efectuate[585]. În ciuda folosirii de măsuri de securitate suplimentare, infracționalitatea legată de acestea este ridicată.

În cazul VISA, spre exemplu, aceste măsuri includ elemente de securitate fizică (folosirea unei holograme, semnătura titularului, repetarea cuvântului Visa în zona de semnătură a cardului), a unui standard de securitate a datelor cardurilor (*Payment Card Industry* (PCI) *Data Security Standard* (DSS)[586]) și de niveluri suplimentare de protecție cum ar fi: *Address Verification Service* (AVS – permite comercianților să verifice adresa folosită de titular în conexiune cu cardul în cauză), *Card Verification Value 2* (CVV2 – un număr de trei cifre imprimat pe spatele cardului, care furnizează o verificare criptografică a informației embosate pe card, pentru a verifica posesia cardului), *Verified by Visa* (VbV – un sistem de autentificare care validează deținerea unui card în timp real în timpul unei tranzacții online) sau *CyberSource Advanced Fraud Screen* (AFS – folosit de

---

[579] *Id.*, p. 17-18.

[580] În situații în care cardul este raportat pierdut, furat sau sunt probleme cu plata sumelor datorate de către deținătorul cardului.

[581] M. MacCarthy, *Information Security Policy in the U.S. Retail Payments Industry*, Stanford Technology Law Review, 3, 2011; vezi și F. Buccafurri și G. Lax, *Implementing disposable credit card numbers by mobile phones*, Electronic Commerce Research, 2011.

[582] Conform Federal Reserve Bank of Boston, *The Survey of Consumer Payment Choice*, consumatorii din SUA dețin 609,8 milioane carduri de credit (ianuarie 2010). Conform Federal Reserve System, op. cit., în anul 2009 au fost efectuate 21,6 miliarde de plăți cu carduri de credit, cu o valoare de 1,9 trilioane dolari.

[583] Conform Consumer Payment Systems, citat în Adam J. Levitin, *Priceless? The economic costs of credit card merchant restraints*, 55 UCLA Law Review 1321, 2008.

[584] La sfârșitul anului 2010, numărul de carduri de debit VISA era de circa 400 milioane, iar numărul de carduri de debit MasterCard era de 123 milioane - conform propriilor site-uri, citate de B. Woolsey și M. Schulz, *Credit card statistics, industry facts, debt statistics*, 2011.

[585] Conform B. Woolsey și M. Schulz, op. cit., la sfârșitul anului 2010, volumul cumpărăturilor VISA era de 1,05 trilioane dolari, iar volumul tranzacțiilor de 28,4 miliarde; volumul cumpărăturilor MasterCard era de 333 miliarde dolari, iar volumul tranzacțiilor de 8,46 miliarde.

[586] Acesta include prevenție, detecție și reacție la incidentele de securitate - vezi detalii la locația https://www.pcisecuritystandards.org/security_standards/.

comercianţii care doresc ca o terţă parte să verifice tranzacţia în cauză)[587], infractorii au început să exploateze în scopuri frauduloase posibilitatea de a folosi carduri de credit sau debit pentru diverse operaţiuni financiare ilegale[588], uneori la scară globală[589], pagubele produse fiind foarte mari[590].

Conform Băncii Centrale Europene[591], la fiecare 2635 plătiţi prin card de credit, un euro este plătit în mod fraudulos, pierderile totale pentru carduri de debit şi credit ajungând, în anul 2012, la peste 1,3 miliarde euro. În SUA, tot în 2012, numărul estimat de tranzacţii neautorizate (numite "third-party fraud") a fost de 31,1 milioane, cu o valoare totală de 6,1 miliarde dolari[592].

Sisteme de cecuri electronice

Prin "cec electronic" se înţeleg mai multe tipuri de tranzacţii electronice[593]. Cele mai des folosite înţelesuri sunt *direct debit* (plată directă dintr-un cont al utilizatorului[594]) şi cecuri care funcţionează similar cecurilor de hârtie, folosind documente XML semnate digital care furnizează un mecanism de autentificare a părţilor la o tranzacţie. Cecurile electronice sunt definite folosind FSML (*Financial Services Markup Langauge*) care permite adăugarea şi ştergerea de părţi din document, semnarea, co-semnarea etc. Semnăturile sunt însoţite de certificate

---

587 VISA, *Global Visa Card-Not-Present Merchant Guide to Greater Fraud Control*, 2009. Vezi şi *Safetech* (tehnologii integrate cu procesarea plăţilor, care permit detectarea unor fraude).

588 Spre exemplu, cazul a 11 persoane care au penetrat sistemele unor comercianţi din USA şi au furat şi vândut circa 40 milioane de numere de carduri de credit şi debit, descris în *Department of Justice Brings Its Largest Identity Theft Action Ever*, The Computer & Internet Lawyer, Vol. 25, No. 10, October, 2008, p. 20-22; arestarea de către FBI a opt persoane care au folosit numere de carduri de credit ale altor persoane pentru a achiziţiona bunuri în valoare de circa un milion dolari, descrisă în *FBI Arrests Eight In Credit Card Fraud*, Cardline, Vol. 10, Iss. 16, 2010, p. 2.

589 Vezi cazul în care, folosind carduri de debit clonate sau furate (la care aveau şi PIN-urile), o grupare infracţională a accesat peste 2100 automate bancare în cel puţin 280 oraşe de pe trei continente şi, în circa 12 ore, au obţinut peste 9 milioane dolari – vezi detalii în FBI, *High-Tech Heist: 2,100 ATMs Worldwide Hit at Once*, disponibil la locaţia http://www.fbi.gov/news/stories/2009/november/atm_111609. Vezi şi cazul Dark Market, în care FBI a folosit un agent sub acoperire, care a rezultat în 56 de persoane arestate în întrega lume: FBI, *'Dark Market' Takedown: Exclusive Cyber Club for Crooks Exposed*, disponibil la locaţia http://www.fbi.gov/news/stories/2008/october/darkmarket_102008. Vezi şi cazul în care o grupare criminal a retras 13 milioane dolari într-o singură zi de la automate bancare din şase ţări, descris în M. Liebowitz, *How cyber crime gang stole $13 million in a day*, http://www.msnbc.msn.com/id/44291945/ns/technology_and_science-security/t/how-cyber-crime-gang-stole-million-day/. A se vedea şi cazul Acme Corp., descris în J. A. Valentine, *Investigating Large-Scale Data Breach Cases*, In J. Bayuk (ed.), *CyberForensics*, Springer's Forensic Laboratory Science Series, 2010.

590 Spre exemplu, M. Pulina şi A. Paba, *A discrete choice approach to model credit card fraud*, 2010; *Organised cybercrime and payment cards*, Card Technology Today, February, 2009; M. Cornish, K. Delpha şi M. Erslon, *Mastercard international security and risk management: Credit card fraud*, 2004.

591 ECB, *New report on card fraud shows online fraud increased in 2012*, 2014.

592 Federal Reserve System, *Federal Reserve Payments Study*, 2013.

593 Electronic Check Council, *Electronic Check: Glossary and acronyms*, 2001.

594 De pildă, eCheck.Net furnizat de Authorize.Net.

emise de bănci care asociază cheia semnatarului unui cont bancar. Încasarea cecurilor este realizată prin intermediul standardelor existente - ANSI X9.46 cu reprezentare FSML în loc de imaginea cecului şi scrisoare cash ANSI X9.37 conţinută în încapsulare X9.46[595].

Sisteme de monedă (cash) electronic

Banii electronici (numiţi în diverse publicaţii *electronic money, digital money, e-money, electronic cash, digital cash, e-currency, electronic currency, digital currency* sau *cyber currency*) pot fi categorizaţi ca fiind stocaţi pe un cip (*card-based*) sau stocaţi pe un server (*software-based*), folosiţi în domeniul comercial standard sau în mediul virtual[596]. Valoarea banilor stocaţi pe un cip este înregistrată pe un cip cu circuit integrat incorporat într-un card de plastic sau un telefon mobil, valoarea fiind administrată de o aplicaţie incorporată.

Un card cu cip este un card de plastic care conţine încorporate un microprocesor capabil să stocheze date şi să execute anumite calcule. În funcţie de tehnologia care o încorporează, aceste carduri pot fi de tip *contact* (cardul trebuie introdus fizic într-un cititor), *fără contact* (cardul trebuie să treacă în apropierea unui cititor), *hybrid* (care combină capacităţile celor două categorii anterioare), *de proximitate* (care comunică printr-o antenă similar cu cardurile fără contact, dar este de tip *read only*, adică nu pot fi scrise informaţii în memoria cip-ului)[597].

Banii electronici *stocaţi pe un server* (*server-based type*) nu necesită un dispozitiv fizic, valoarea este înregistrată şi administrată pe un server al furnizorului de servicii de bani electronici (acestea au existat mai mult ca un fel de proiecte pilot, nefiind cu adevărat răspândite[598]). Un exemplu de portofel electronic este Google Wallet, o aplicaţie disponibilă pentru un telefon mobil, care permite stocarea de versiuni virtuale ale cardurilor de plastic.

Banii folosiţi în mediul virtual sunt reprezentaţi de date informatice[599] şi implică un lanţ de semnături digitale (fiecare deţinător transferă moneda către o altă entitate prin semnare digitală adăugată la sfârşitul şirului care reprezintă moneda)[600]. Astfel de bani pot fi expresii numerice ale unor monede existente sau pot fi monede digitale sau Internet, folosite în mediul virtual prin intermediul unui browser, al poştei electronice sau al mesajelor text de pa un telefon mobil[601] (spre

---

595 Vezi http://searchdatamanagement.techtarget.com/answer/What-are-e-checks.

596 P. Athanassiou şi N. Mas-Guix, *Electronic money institutions: Curent trends, regulatory issues and future prospects*, 2008.

597 Pentru detalii, P. Athanassiou şi N. Mas-Guix, op. cit., p. 8.

598 European Central Bank, *E-payments in Europe – The Eurosystem's perspective*, 2002.

599 J. Camenisch, S. Hohenberger şi A. Lysyanskaya, *Compact E-Cash*, 2006.

600 S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009.

601 Unele monede electronic au fost suspendate pentru încălcarea unor legi – vezi cazul *e-gold*, operată de Gold & Silver Reserve Inc. sub denumirea e-gold Ltd. în plângerea penală USA v. E-Gold, Ltd., Gold & Silver Reserve, Inc., Douglas L. Jackson, Barry K. Downey şi Reid A. Jackson pentru violarea 18 U.S.C. § 1956 (*Conspiracy to Launder Monetary Instruments*); 18 U.S.C. § 371 (*Conspiracy*); 18 U.S.C. § 1960 (*Operation of Unlicensed Money Transmitting Business*); D.C. Code § 26-1002 (*Money Transmitting Without a License*) şi 18 U.S.C. § 2 (*Aiding and Abetting and Causing an Act to be Done*) şi 18 U.S.C. § 982 (a)(1) (*Criminal Forfeiture*).

BCU IASI CENTRAL UNIVERSITY LIBRARY

exemplu, WebMoney[602], Digital Gold Currency[603], Bitcoin[604] etc.[605]). Există un număr de procesori de plăţi electronice (spre exemplu, PayPal, Google Checkout[606], Authorize.Net[607], Skrill etc.). Conform Bank of Japan[608], valoarea banilor electronici emişi şi folosiţi este mică în comparaţie cu plăţile cu numerar sau cu carduri de credit[609].

B. Conţinutul constitutiv al infracţiunii cuprinde: a) latura obiectivă şi b) latura subiectivă.

a) **Latura obiectivă** cuprinde elementul material, cerinţe esenţiale, urmarea imediată şi legătura de cauzalitate.

Elementul material al laturii obiective se poate realiza prin oricare din următoarele trei acţiuni alternative prevăzute de legiuitor:

Efectuarea unei tranzacţii electronice prin utilizarea frauduloasă a unui instrument de plată electronică sau a datelor de identificare ale instrumentului de plată electronică, fără consimţământul titularului. În ceea ce priveşte această primă variantă normativă, sunt prevăzute ca *cerinţe esenţiale*: operaţiunea frauduloasă să implice un instrument de plată electronică sau datele de identificare ale acestuia, precum şi lipsa de consimţământ al titularului instrumentului de plată electronică.

O altă acţiune alternativă constă din *efectuarea unei tranzacţii electronice prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive*. În cazul acestei variante, *cerinţa esenţială* este ca efectuarea operaţiunilor din alin. (1) să se realizeze fie prin utilizarea neautorizată a oricăror date de identificare, fie ca datele utilizate să fie fictive.

Transmiterea neautorizată către altă persoană a oricăror date de identificare pentru realizarea uneia dintre operaţiunile de mai sus. În ceea ce priveşte această ultimă modalitate, pentru că nu se face menţiunea cu privire la mijloacele prin care pot fi transmise neautorizat datele de identificare către alte persoane, poate fi vorba de orice mijloace de transmitere la distanţă, precum şi

---

602 WebMoney este o monedă electronică şi un sistem de plată online deţinut şi administrat de WM Transfer Ltd., cu sediul în Belize. Fiecare cont este numit „poşetă" şi este denominat în echivalent aur, dolari americani, euro etc.

603 DGC este o formă de monedă electronică bazată pe uncia de aur.

604 Vezi www.bitcoin.org. Vezi riscurile implicate în Kaspersky Lab, *IT Threat Evolution: Q2 2011*, 2011 şi D. Coldewey, *$250,000 worth of Bitcoins stolen in net heist*, 2014.

605 Dove Consulting, *The Electronic Payments Study*, Study Research Sponsored by the Federal Reserve System, 2008.

606 Serviciu de procesare a plăţilor online: utilizatorii stochează cardurile lor de debit sau credit şi informaţia privind livrarea bunurilor pe contul lor Google, putând plăti la comercianţii participanţi printr-un click pe un buton de pe ecran.

607 Intermediar de servicii de plată electronică; permite comercianţilor acceptarea de plăţi prin intermediul cardurilor de credit sau al cecurilor electronice prin intermediul site-ului web.

608 Bank of Japan, *Recent Developments in Electronic Money in Japan*, 2008.

609 Nomura Research Institute, *Electronic money trends as revealed by a consumer survey*, 2009; H. Fujiki şi M. Tanaka, *Demand for Currency, New Technology and the Adoption of Electronic Money: Evidence Using Individual Household Data*, 2009. Vezi şi J.-M. Sahut, *The Adoption and Diffusion of Electronic Wallets: The Case of Monéo*, Journal of Internet Banking and Commerce, Vol. 13, No.1, April, 2008.

BUCHAREST UNIVERSITY LIBRARY

transmiterea din mână în mână. Ceea ce se prezintă ca o *cerință esențială* este ca utilizarea instrumentului de plată electronică să fie făcută neautorizat.

Efectuarea de operațiuni financiare în mod fraudulos este o infracțiune care prezintă numeroase și variate posibilități de realizare, infractorii în domeniu s-au dovedit extrem de inventivi în această privință. Pentru o cunoaștere în profunzime a modalităților normative prevăzute de legiuitor, vom prezenta în continuare aspecte practice esențiale privind efectuarea de operațiuni financiare în mod fraudulos.

Cardurile de credit sau debit pot fi obținute ilegal în mod fizic printr-o operație falsă (*new account fraud*[610]), bazată pe furtul de identitate (*identity takeover* sau *identity usurpation*)[611], ori prin furtul fizic al unui card (după ce a intrat în posesia titularului sau înainte, prin sustragerea acestuia din interiorul firmelor de curierat sau autovehiculele acestora, din cutia poștală a titularului sau prin devierea corespondenței) sau prin găsirea de carduri pierdute. În situația în care infractorii au acces fizic la un card, acesta poate fi contrafăcut (clonat). Des întâlnite sunt infracțiunile prin folosirea mijloace electronice sau telefonice (*card not present*[612]).

Datele cardurilor de credit sau debit pot fi obținute virtual prin cooperarea involuntară a deținătorilor cardurilor (*phishing*), prin citirea fizică a datelor de pe carduri fără știința deținătorului (*skimming* sau copiere[613]), prin *acces ilegal* la sisteme informatice unde acestea sunt stocate, ori capturarea datelor din memoria volatilă (folosind un *RAM scrapper*, care poate captura datele cardului din memoria volatilă, unde nu este criptată[614]), prin traficul pe Internet de astfel de date (*carding*) sau prin intermediul programelor informatice malițioase (*malware*).

Skimming-ul presupune copierea întregului conținut al înregistrărilor de pe banda magnetică[615] a unui card autentic, de regulă în timp ce este folosit pentru o

---

610 Conform unui studiu citat în C. J. Hoofnagle, *Internalizing identity theft*, UCLA Journal of Technology Law, Vol. 13, Issue 2, Fall, 2009, în anul 2005, între 1,2 și 2,8 milioane de americani au fost victime ale acestui tip de fraudă. Vezi și L. Delamaire, H. Abdou și J. Pointon, *Credit card fraud and detection techniques: A review*, Banks and Bank Systems, vol. 4, Iss. 2, 2009.

611 Conform Federal Trade Commission, *The Consumer Sentinel Network* (2010), frauda cu carduri de credit a fost cea mai des întâlnită formă de furt de identitate. Vezi discuții pe această temă în B.-J. Koops și Z. Geradts, *Identity-Related Crime and Forensics*, 2009; H. M. Howard, *The negligent enablement of imposter fraud: A common–sense common law claim*, Duke Law Journal, Vol. 54, 2005; J. Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Fishing Attacks*, 20 Berkeley Technology Law Journal, 259, 2005.

612 O tranzacție de tip *card not present* (CNP) se desfășoară prin telefon sau prin mijloace electronice, folosind Internetul. Vezi cazuri de fraude tip CNP în A. Passman, *Card Not Present Is Very Present In Fraud*, Credit Union Journal, vol. 15, Iss. 31, 2011; S. Bell, *Mobile Merchants Experiencing Most Card-Not-Present Fraud*, Cardline, vol. 10, 42, 2010, p. 1.

613 Vezi United States v. Keita, No. 12-4957 (4th Cir. Feb. 6, 2014); United States v. Lall, 607 F.3d 1277 (11th Cir. 2010); People v. Bivens, H029609 (Cal. Ct. App. Oct. 10, 2007).

614 *2011 Data breach investigations report*, op. cit.

615 Conform standardului ISO/IEC 7811, banda magnetică conține trei piste, care stochează numărul de cont asociat cu cardul, un cod de țară, numele deținătorului cardului, data expirării și, opțional, alte date privind deținătorul cardului (spre exemplu, adresa acestuia).

BCU IASI / CENTRAL UNIVERSITY LIBRARY

tranzacţie licită (*Electronic Data Capture*, trecerea cardului printr-un cititor electronic). Cel mai adesea această metodă este folosită la puncte de vânzare (*Point-of-Sale Transactions*[616] sau POS) cum ar fi benzinării[617], marile magazine[618] sau restaurante[619] sau la ATM-uri (care implică o cameră ascunsă pentru înregistrarea PIN-ului[620] şi o tastatură falsă, plasată peste cea reală, pentru a înregistra ceea ce se tastează)[621]. În unele cazuri, dispozitive de citire au fost plantate înainte de a fi trimise de la fabricant la destinaţie[622] sau făptuitorii au pretins că au de ajustat terminalul POS[623].

Chiar cardurile cu RFID (*radio frequency identification*)[624], care sunt folosite fără contact fizic (*contactless*[625]), sunt susceptibile la o formă de *skimming virtual*. Cel care copiază datele (*skimmer*-ul), le poate folosi ulterior pentru a contraface carduri sau le poate vinde altor indivizi interesaţi. *Skimming*-ul presupune copierea întregului conţinut al înregistrărilor de pe banda magnetică[626] a unui card autentic, de

---

616 Tranzacţii în persoană (*face-to-face*), în care deţinătorul foloseşte cardul la locaţia comerciantului. Vezi cazul în care sistemul Vacationland Vendors care procesează tranzacţiile cu carduri a fost penetrat, descris la locaţia http://www.cio.com/article/689742 /Vending_Machine _Company_Announces_Major_Data_Breach.

617 Conform *House of cards*, Consumer Reports Magazine, June, 2011, atacurile de tip *skimming* au atins un nivel în Florida încât autorităţile au sugerat consumatorilor folosirea de monetar pentru a plăti benzina cumpărată.

618 Spre exemplu, cazul în care 80 de magazine Michaels, din 20 de state americane, au fost victime ale unei astfel de scheme de obţinere a datelor cardurilor de credit şi debit, raportat în *Michaels stores hit by card skimming*, Consumer Reports Magazine, 13 mai 2011.

619 Spre exemplu, cazul în care trei persoane au furnizat chelnerilor unui restaurant dispozitive de copiere a cardurilor (*skimmer*), descris în *Three men charged with card skimming*, Cardline, vol. 9, Iss. 42, 2009, p. 1.

620 Conform unor cercetători de la University of California, San Diego, folosirea unei camera termale montată deasupra tastaturii ATM-ului permite detectarea numerelor tastate – vezi *Thermal Cameras Use Heat to Steal ATM PINs*, http://www.securitynewsdaily.com/thermal-cameras-use-heat-to-steal-atm-pins-1068/

621 Spre exemplu, cazul unor bulgari care au instalat astfel de echipamente la ATM-uri în New York City şi alte cazuri raportate de FBI la locaţia http://www.fbi.gov/news/stories/2011/july /atm_071411.

622 Vezi cazul raportat în SANS, *NewsBites*, 10 (81), 2008, în care o organizaţie criminală, cu membrii în China şi Pachistan, a plantat astfel de dispozitive în automate trimise în ţari cum ar fi Anglia, Irlanda, Danemarca, Belgia sau Olanda. Informaţiile astfel obţinute erau transmise prin telefoane mobile unor persoane din Pachistan, care efectuau retrageri de numerar şi cumpărături frauduloase. Atacut al durat nouă luni, pagubele produse fiind de 50-100 milioane dolari.

623 VISA, *New POS Tamper Scheme*, 2007.

624 Conform unui raport, în USA există 35 milioane astfel de carduri; datele acestui tip de card pot fi obţinute chiar aflate în buzunarul sau poşeta titularului. De remarcat că folosirea în aceste cazuri este posibilă doar o dată, deoarece codul de securitate folosit în plăţile cu aceste carduri se schimbă la fiecare folosire - vezi un articol despre această metodă de obţinere a datelor unui card în *Newer cards can be hijacked, too*, Consumer Reports Magazine, June, 2011.

625 Aceste carduri nu transmit numele deţinătorului şi adaugă un cod criptat la mesajul de plată, ceea ce face comiterea de fraude mult mai dificilă - vezi în R. J. Sullivan, *The changing nature of U.S. card payment fraud: Issues for industry and public policy*, 2010.

626 Conform standardului ISO/IEC 7811, banda magnetică conţine trei piste, care stochează numărul de cont asociat cu cardul, un cod de ţară, numele deţinătorului cardului, data expirării şi, opţional, alte date privind deţinătorul cardului (spre exemplu, adresa acestuia).

BCU IASI / CENTRAL UNIVERSITY LIBRARY

regulă în timp ce este folosit pentru o tranzacţie licită (*Electronic Data Capture*, trecerea cardului printr-un cititor electronic sau terminal).

Infractorii profesionişti pot obţine numere de carduri de credit în mod direct prin accesarea ilegală a unor site-uri sau sisteme informatice unde astfel de date sunt stocate[627]. Prin intermediul unor site-uri specializate, criminalii tranzacţionează informaţii privind datele cardurile de credit sau debit[628] şi chiar oferă carduri contrafăcute pentru vânzare (aşa-numita activitate de *carding*[629]; există şi indivizi care folosesc Internetul în vederea diseminării sau tranzacţionării pe scară largă a informaţiilor privind cardurile de credit sau debit sunt denumiţi *carderi*[630]). O altă modalitate de obţinere a detaliilor bancare ale unui card de credit este utilizarea contaminanţilor informatici (spre exemplu, un *keystroke logger* sau un *password stealer*). Criminalii pot instala programe maliţioase pe site-uri legitime sau pot infecta telefoane mobile (*smartphone*)[631].

În ceea ce priveşte banii electronici stocaţi pe un card cu cip, un caz de fraudă este raportat de Bank of Japan (folosirea unui card de credit furat, pentru a încărca o anumită valoare de bani electronici). În acest caz, problema nu a fost legată de funcţionarea sistemelor de securitate a serviciului în sine, ci, un proces insuficient de autentificare a utilizatorului realizat la înregistrarea informaţiei

---

627 Spre exemplu, cazul TJX, care, în anul 2007, a raportat o intruziune în sistemele sale informatice ce a rezultat în compromiterea a zeci de milioane de carduri de credit, descris la locaţia http://www.tjx.com/TJX_press_release_Jan_17_%2007.pdf.

628 Departamentul Justiţiei din SUA prezintă pe site-ul www.cybercrime.gov numeroase cazuri, dintre acestea menţionăm: Între februarie 2008 şi mai 2009, Juan Javier Cardenas a obţinut şi traficat numere de carduri de credit furate cu intenţia de a frauda (agenţii Secret Service au găsit 26.669 numere de carduri de credit stocate pe calculatorul acestuia). În 2009, Secret Service a găsit la Rogelio Hackett Jr.'s peste 675.000 numere de carduri de credit furate, obţinute fie prin accesarea fără drept a reţelelor informatice ale comercianţilor sau prin intermediul forumurilor de carding pe Internet; acesta vindea informaţiile cardurilor de credit sau fabrica şi vindea carduri contrafăcute, pagubele produse depăşind 36 milioane dolari.

629 Spre exemplu, cazul *Shadowcrew*, descris în K. Kiefer Peretti, *Data breaches: What the underground world of "carding" reveals*, Santa Clara Computer and High Technology Law Journal, Vol. 25, 2009: este vorba despre o organizaţie criminală globală, cu mii de membrii, dedicată promovării şi facilitării furtului de carduri de credit şi debit şi furtului de informaţii personale. Organizaţia opera un site pe Internet şi avea o structură ierarhică ce includea următoarele roluri: administratori (un fel de consiliu guvernator), moderatori, referenţi, comercianţi şi membrii. Membrii acestei reţele au traficat colectiv peste 1,5 milioane de carduri de credit furate şi au produs peste 4 milioane de dolari pierderi pentru instituţiile financiare emitente. Vezi şi *Carderplanet*, *International Association for the Advancement of Criminal Activity* (IAACA), ulterior devenite *the Theft Services*, *CardersMarket* şi *CcpowerForums*, descrise în aceeaşi lucrare.

630 Vezi cazul unui individ care cumpăra carduri de credit prin Internet de la indivizi care se crede că erau în Rusia, pentru a le revinde în New York, New Jersey şi Washington, D.C. Conform informaţiilor publicate, au fost raportate peste 4.400 utilizări frauduloase, totalizând 770.674 dolari – vezi US Department of Justice, Press Release August 10, 2011. Într-un alt caz, un individ a fost condamnat la 14 ani închisoare, plata a 2,8 milioane dolari restituiri şi o amendă de 250.000 dolari pentru operarea unei scheme online (*carding forum*) prin care vindea carduri de credit contrafăcute - US DoJ, Press Release September 9, 2011.

631 Spre exemplu, cazul Zeus Mitmo, descris la locaţia http://www.enisa.europa.eu/act/application-security/smartphone-security-1/top-ten-risks/financial-malware-attacks/?searchterm=credit%20card

privind cardul de credit[632]). În ceea ce privește banii electronici stocați pe un server, riscul privind apariția cazurilor de fraudă este mai ridicat, putând exista cazuri de folosire neautorizată a serviciului (impersonare sau hacking), serviciul fiind furnizat de la distanță, mai ales via Internet.

Un caz de fraudă a implicat alterarea unui mesaj electronic privind valoarea unui transfer de credit la încărcarea valorii banilor electronici online (adică, valoarea creditată în contul bancar al furnizorului serviciului a fost diminuată față de valoarea încărcată). Un alt caz a implicat folosirea neautorizată a unui identificator (ID), care poate fi atribuită direct măsurilor de securitate informatică insuficiente la nivelul serverului care stochează datele privind banii electronici[633].

Urmarea imediată, nu constă din producerea unei pagube, fiind suficientă producerea unei stări de pericol pentru desfășurarea în condiții de securitate a activităților de comerț electronic.

Legătura de cauzalitate dintre elementul material și urmarea imediată rezultă implicit din săvârșirea acțiunilor descrise în norma de încriminare (*ex re*).

b) Latura subiectivă cuprinde: elementul subiectiv și cerințe esențiale.

Elementul subiectiv. Infracțiunea de efectuare de operațiuni financiare în mod fraudulos se săvârșește cu intenție directă, ceea ce rezultă clar din conținutul art. 250 din noul Cod penal.

Forme. Modalități. Sancțiuni

A. Forme

Infracțiunea, fiind una comisivă și intenționată, se poate prezenta sub oricare dintre formele sale: acte de pregătire, tentativa, consumarea și epuizarea.

a) **Actele de pregătire** nu sunt incriminate și ca atare nepedepsibile

b) **Tentativa** este posibilă și se pedepsește în conformitate cu prevederile art. 252 din noul Cod penal.

c) **Consumarea** acestei infracțiuni are loc în momentul în care oricare dintre operațiunile financiare frauduloase menționate de articolul analizat (spre exemplu, când s-a realizat efectuarea de transferuri de fonduri, în afara celor ordonate de către instituțiile financiare, sau când s-au realizat activități frauduloase de retrageri de numerar, încărcarea sau descărcarea unui instrument de plată electronică).

d) **Epuizare.** Fapta se poate prezenta și sub formă continuată, **epuizarea** având loc în aceste situații când au încetat actele de prelungire ale activității incriminate (efectuări de operațiuni frauduloase cu mijloace de plată electronice).

B. Modalități

a) **Modalitățile normative simple** sunt cele trei arătate în textul de lege:

- Efectuarea unei tranzacții electronice prin utilizarea frauduloasă a unui instrument de plata electronică sau a datelor de identificare ale instrumentului de plată electronică, fără consimțământul titularului.

---

632 Bank of Japan, *Recent Developments in Electronic Money in Japan*, 2008.

633 *Id.*

- Efectuarea unei tranzacţii electronice prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.
- Transmiterea neautorizată către altă persoană a oricăror date de identificare pentru realizarea uneia dintre operaţiunile de mai sus.

b) **Modalităţi de fapt.** Aşa cum am arătat la analiza elementului material al laturii modalităţile de fapt se pot prezenta faptic într-o mare variate de acţiuni în raport cu situaţiile concrete.

C. **Sancţiuni**

Prevăzută de lege pentru infracţiunea de efectuare de operaţiuni financiare în mod fraudulos în variantele de la alin. (1) şi (2) este închisoare de la 2 la 7 ani, iar pentru cea de la alin. (3) este închisoare de la unu la 5 ani.

Explicaţii complementare

Aspecte procesuale: Acţiunea penală se pune în mişcare din oficiu. Competenţa de judecată în primă instanţă revine judecătoriei.

Referinţe de drept comparat

Având în vedere faptul că, în ceea ce priveşte comerţul electronic şi mijloacele de plată electronice, există un complex cadru legal european (a se vedea explicaţiile date în cadrul analizei), cu obligaţii pentru statele membre de a adopta măsuri penale de protecţie a relaţiilor în acest domeniu, există reglementări similare în statele membre ale UE, iar datorită expunerii globale a tranzacţiilor electronice, şi în numeroase state la nivel mondial.

4.4.4 Acceptarea operaţiunilor financiare efectuate în mod fraudulos

Art. 251. (1) Acceptarea unei operaţiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, cunoscând că este efectuată prin folosirea unui instrument de plată electronică falsificat sau utilizat fără consimţământul titularului său, se pedepseşte cu închisoare de la unu la 5 ani.
(2) Cu aceeaşi pedeapsă se sancţionează acceptarea uneia dintre operaţiunile prevăzute în alin. (1), cunoscând că este efectuată prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.

Concept şi caracterizare

Vechiul Cod penal nu prevedea această infracţiune, ea fiind preluată în noul Cod penal din Legea nr. 365/2002[634], art. 28, cu aceeaşi denumire marginală: *Acceptarea operaţiunilor financiare efectuate în mod fraudulos*. Există o singură

[634] Legea nr. 365/2002 privind comerţul electronic, Capitolul VIII - Infracţiuni săvârşite în legătură cu emiterea şi utilizarea instrumentelor de plată electronică şi cu utilizarea datelor de identificare în vederea efectuării de operaţiuni financiare.

BCU IASI CENTRAL UNIVERSITY LIBRARY

modificare, pe care o considerăm neinspirată, anume reducerea limitei maxime a pedepsei (de la 12 ani la 5 ani), în total dezacord cu cerințele existente la nivelul Uniunii Europene sau la nivel global. Cheia eficienței luptei împotriva fraudei în domeniul instrumentelor de plată electronice constă într-o politică penală care prevede pedepse eficiente, disuasive și proporționale cu gravitatea acestor fapte[635].

La art. 1, pct. 11 din lege[636], la care se face referire în art. 28, este prevăzută definiția instrumentului de plată electronică și operațiunile care pot fi realizate cu acesta; asemenea operațiuni sunt incriminate dacă se realizează în condițiile prevăzute în art. 28 din legea care prevede infracțiunea de acceptare a operațiunilor financiare efectuate în mod fraudulos.

Legiuitorul român, pentru a ajunge la formularea din art. 251 a combinat două texte din Legea nr. 365/2002 (art. 1, pct. 11 și art. 28) și anume:

A. Acceptarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, cunoscând că este efectuată prin folosirea unui instrument de plată electronică falsificat sau utilizat fără consimțământul titularului său, se pedepsește cu închisoare de la unu la 5 ani.

B. Acceptarea uneia dintre operațiunile prevăzute în alin. (1), cunoscând că este efectuată prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.

Reglementarea din Legea nr. 365/2002 are ca origine Decizia-cadru a Consiliului din 28 mai 2001 de combatere a fraudei și a falsificării mijloacelor de plată, altele decât numerarul[637]. În această Decizie se arată, în partea introductivă (pct. 9) că este necesar ca aceste forme de comportament să fie clasificate ca infracțiuni în toate statele membre și ca astfel de fapte să facă obiectul unor sancțiuni eficace, proporționale și cu efect de descurajare care să fie aplicate

---

[635] Council Framework Decision 2001/413/JHA of 28 May 2001 - *Combating fraud and counterfeiting of non-cash means of payment*, OJ L 149, 2.6.2001, p. 1, care cerea statelor membre să incrimineze frauda cu mijloace de plată electronice și să stabilească pedepse penale efective, proporționale și care să descurajeze săvârșirea unor astfel de fapte, incluzând pedepse cu închisoarea care să permită extrădarea. Comisia Europeană a prezentat încă din aprilie 2004 două rapoarte cu măsurile luate de statele membre în care se analiza modul în care s-au conformat cu cadrul cerut de această decizie. Mulți factori de decizie în domeniu consideră că unele state au încă un nivel redus al pedepselor pentru acest tip de fraude. A se vedea și European Commission, 30.4.2004, Report of the Commission based on Article 14 of the Council Framework Decision of 28 May 2001 - *Combating fraud and counterfeiting of non-cash means of payment*, COM(2004) 346 final; 20.2.2006, Second report based on Article 14 of the Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, COM(2006)65 final. De asemenea, Europolul a semnalat, încă din anul 2005, că legile naționale în domeniu sunt extrem de permisive în ceea ce privește frauda, acest lucru nefăcând decât să constituie o adevărată invitație pentru crima organizată să se îndrepte spre acest fenomen criminal, din ce în ce mai profitabil și mai sigur, considerat arhetipul de infracțiune "risc-redus, profit-crescut" – a se vedea Europol, *EU Organised Crime Report* (Public Version), 2005, p. 7 și 32.

[636] Art. 1, pct. 11 din Legea nr. 365/2002 prevede ce este instrumentul de plată electronică.

[637] Council Framework Decision 2001/413/JHA din 28 mai 2001, OJ L 149, 2.6.2001.

BCU IASI CENTRAL UNIVERSITY LIBRARY

persoanelor fizice şi juridice care au săvârşit sau care răspund pentru săvârşirea unor asemenea infracţiuni[638].

Elemente preexistente

A. Obiectul juridic al acestei infracţiuni este reprezentat în principal de relaţiile sociale a căror formare, desfăşurare şi dezvoltare au în vedere protejarea interesului economico-financiar al titularului de drept al instrumentului de plată electronică sau al monedei electronice. În al doilea rând, sunt ocrotite relaţiile privind securitatea activităţilor de comerţ electronic şi cele privind încrederea în aceste categorii de instrumente de plată. În al treilea rând, sunt protejate şi relaţiile sociale privitoare la viaţa privată a titularului instrumentului de plată electronică (în cazurile în care este vorba de furtul de identitate)[639].

B. Obiectul material. Infracţiunea nu prezintă un obiect material deoarece activitatea interzisă prin norma de incriminare nu se răsfrânge asupra unei entităţi materiale.

C. Subiecţii infracţiunii

a) Subiectul activ al acestei infracţiuni este unul calificat. Acesta poate fi o persoană care îndeplineşte condiţiile generale pentru a răspunde penal şi care are atribuţii de acceptare de operaţiuni financiare în mod curent, în virtutea atribuţiilor sale de serviciu[640] sau de efectuare de operaţiuni de transfer de fonduri, altele decât cele ordonate sau executate de instituţii financiare, retrageri de numerar, încărcare şi descărcare a unui instrument de plată electronică (subiectul activ este adesea un funcţionar cu sarcini de decizie din cadrul instituţiilor cu atribuţii în domeniul vizat).

Astfel, una dintre aceste persoane poate fi comerciantul acceptant; acesta, în conformitate cu Regulamentul BNR nr. 6/2006, art. 1, pct. 8, este entitatea care acceptă cardul sau instrumentul de tip monedă electronică (*e-money*) ca mijloc de plată, pe baza unui contract încheiat anterior cu o instituţie acceptantă. În sensul acestui regulament, sunt asimilate comercianţilor acceptanţi şi entităţile care nu au calitatea de comerciant.

În categoria celor care acceptă operaţiunile la care face referire textul de lege şi care pot fi subiect activ al acestei infracţiuni sunt şi cei care fac parte din instituţia acceptantă. În conformitate cu prevederile legale aceasta este o instituţie de credit sau o instituţie financiară nebancară care oferă comercianţilor acceptanţi

---

638 Vezi categoriile de infracţiuni şi definirea lor în art 2, 3 şi 4 din Decizia-cadru a Consiliului din 28 mai 2001 de combatere a fraudei şi a falsificării mijloacelor de plată, altele decât numerarul.

639 Acceptarea operaţiunilor financiare efectuate în mod fraudulos este o infracţiune care aduce atingere relaţiilor sociale privind dreptul la o viaţă privată neperturbată, drept prevăzut şi protejat de Convenţia europeană de salvgardare a drepturilor omului şi a libertăţilor fundamentale; a se vedea: Art. 18 al Convenţiei europene de salvgardare a drepturilor omului şi a libertăţilor fundamentale: *restricţiile care, potrivit prezentei convenţii, sunt aduse respectivelor drepturi şi libertăţi, nu pot fi aplicate decât în scopul pentru care ele au fost prevăzute.*

640 Regulament nr. 6 din 11 octombrie 2006, publicat în M. Of. nr. 927 15 noiembrie 2006, cu intrare în vigoare la 15 noiembrie 2006, privind emiterea şi utilizarea instrumentelor de plată electronică şi relaţiile dintre participanţii la tranzacţiile cu aceste instrumente.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

servicii de acceptare la plată a cardurilor şi/sau a instrumentelor de plată de tip monedă electronică (*e-money*), în baza unui contract încheiat în prealabil între aceasta şi comerciantul acceptant. De asemenea, oferă servicii de eliberare de numerar la ghişeele sale şi în reţeaua proprie de terminale deţinătorilor.

În cazul instrumentelor de plată electronică de tipul cardului, instituţia acceptantă poate fi şi emitentul instrumentului de plată. În cazul instrumentelor de plată electronică cu acces la distanţă de tipul home-banking, internet-banking sau mobile-banking, instituţia acceptantă este întotdeauna şi emitentul instrumentului de plată electronică respectiv, aceasta furnizând serviciile specifice acestor instrumente de plată electronică numai deţinătorilor[641].

De asemenea, pot intra în categoria subiecţilor activi şi procesatorii în domeniul instrumentelor de plată electronică, aceştia fiind definiţi de lege ca fiind persoane juridice ce acţionează în cadrul schemelor de plăţi cu carduri, ca intermediar între deţinător, comerciantul acceptant, emitent, instituţie acceptantă, alt procesator şi/sau altă persoană juridică, în baza unui contract încheiat cu emitentul/instituţia acceptantă, pentru a facilita transmiterea şi prelucrarea tranzacţiilor rezultate prin utilizarea acestor instrumente de plată electronică[642].

b) Subiectul pasiv este persoana fizică sau juridică al cărei patrimoniu este afectat prin acceptarea operaţiunilor efectuate în mod fraudulos. De observat că toate operaţiunile subiectului activ se fac pe seama subiectului pasiv, adică al unei persoane fizice sau juridice care suferă consecinţele materiale ale operaţiilor de mai sus. Interesul subiectului activ ar fi să obţină avantaje materiale prin operaţiile financiare.

Structura şi conţinutul juridic al infracţiunii

Aceasta este alcătuită din situaţie premisă şi conţinutul constitutiv al infracţiunii.

A. Situaţia premisă

Pentru ca infracţiune de acceptare a operaţiunilor financiare frauduloase să poată fi săvârşită, trebuie să existe o situaţie premisă, anume existenţa de operaţiuni financiare frauduloase cu mijloace de plată electronice, de a căror existenţă făptuitorul ştie şi le acceptă, în oricare din formele pe care le descrie legiuitorul în cele trei modalităţi normative.

B. Conţinutul constitutiv cuprinde: a) latura obiectivă şi b) latura subiectivă a infracţiunii.

a) Latura obiectivă cuprinde elementul material, cerinţe esenţiale, urmarea imediată şi legătura de cauzalitate.

Elementul material constă în acţiunea de acceptare a operaţiunilor financiare frauduloase, acţiune prezentată de legiuitorul penal în următoarele trei modalităţi normative alternative:

- Acceptarea unei operaţiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de

[641] Art. 1, pct. 11 din Regulamentul BNR nr. 6/2006.
[642] *Id.*, art. 1, pct. 16.

fonduri, cunoscând că este efectuată prin folosirea unui instrument de plată electronică falsificat;

- Acceptarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, cunoscând că este efectuată prin folosirea unui instrument de plată electronică, utilizat fără consimțământul titularului său;
- Acceptarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, cunoscând că este efectuată prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.

Cerințe esențiale. În cazul primei modalități normative, prevăzute în cadrul primului alineat al art. 251, cerința esențială pentru existența infracțiunii sub acest aspect este ca făptuitorul să știe că instrumentul de plată era falsificat. În cazul celei de-a doua modalități, prevăzute tot în primul alineat al articolului, este ca instrumentul de plată să fie utilizat *fără consimțământul titularului*. În cazul celei de-a treia modalități, prevăzută în alin. (2) al art. 251, cerința esențială este ca acceptarea operațiunilor prevăzute în primele două modalități de către făptuitor să se facă *cu știința* acestuia despre efectuarea operațiunilor prin utilizarea neautorizată de date de identificare sau prin utilizarea de date de identificare fictive.

Acceptarea de operațiuni financiare efectuate în mod fraudulos prezintă numeroase și variate posibilități de realizare în practică. Astfel, în legătură cu tipul celui care acceptă operațiunile arătate, sunt cunoscute următoarele modalități practice și anume *frauda la comerciant* și *frauda funcționarului instituției financiare.*

Prin **frauda la comerciant** se înțelege acceptarea cardurilor de credit pentru tranzacții frauduloase, unii comercianți colaborând cu alți infractori. În general, este vorba de fraude anterioare blocării cardului, scopul urmărit prin operații fiind sporirea veniturilor, folosind una din următoarele tactici:

- ***Înțelegere secretă*** (*Collusion*): În astfel de cazuri, comercianții, pe baza unei înțelegeri secrete cu alți infractori, folosesc carduri obținute în mod fraudulos, pentru tranzacții fictive. Într-un astfel de caz, anchetat de FBI, după ce au obținut un număr de carduri de credit în mod fraudulos, un număr de făptuitori au conlucrat cu câțiva comercianți care aveau facilități de procesare a cardurilor de credit. Pentru o sumă, numită *kkang fee*, acești comercianți foloseau cardurile respective pentru plăți, fără realizarea unor tranzacții efective. După ce sumele de bani intrau în conturile lor, aceștia plăteau partea "cuvenită" celor care obținuseră fraudulos cardurile[643].
- ***Factoring***[644]: Principiul de funcționare constă în crearea de plăți multiple pe baza unei singure tranzacții reale (duplicare). Acest lucru poate fi făcut

[643] *Two Plead Guilty to Roles in Large-Scale Identity Theft Ring*, http://www.fbi.gov/newark/press-releases/2011/two-plead-guilty-to-roles-in-large-scale-identity-theft-ring.

[644] Contractul de factoring sau facturaj este un contract comercial de creditare la care participă o societate specializată (societate bancară sau o instituție financiară specializată) în încasarea de

BCU IASI CENTRAL UNIVERSITY LIBRARY

prin imprimarea multiplă de chitanţe, în loc de una, sau, la terminalele de plată, prin tastarea sau cererile de autorizare multiple pentru o singură tranzacţie.

- ***Falsificarea***: Semnătura posesorului legitim al cardului poate fi falsificată, încât să arate ca cea originală. Tranzacţiile efectuate de către comerciant pot fi semnate apoi, ca şi cum plăţile fictive (nici un serviciu sau bun nu este furnizat) ar fi aprobate de către posesorul cardului. Sumele efective ale tranzacţiilor pot fi modificate de către un comerciant, spre exemplu prin adăugarea unei cifre la total. În unele situaţii posesorul cardului semnează această sumă (spre exemplu, în situaţia în care suferă de efectele unei intoxicaţii, într-un club sau bar), care duce la o situaţie greu de contestat de către posesorul cardului.
- ***Ameninţarea/Ademenirea***: Semnătura cumpărătorului poate fi, de asemenea, obţinută prin intermediul ameninţării sau al altui tip de manipulare. Din nou, astfel de cazuri sunt greu de dovedit de către victimă.
- ***Smurfing***[645]: Comerciantul sau un angajat este implicat în mod activ (pe cont propriu sau împreună cu unul sau mai mulţi fraudatori) în acceptarea cardurilor blocate la terminalele off-line pentru diferite tranzacţii fictive care generează venituri ilegale.
- ***Firma fantomă/paravan*** (*front store*): Aplicantul caută afilierea la un program de plată prin cărţi de credit în scopul de a efectua tranzacţii ilegale cu carduri de credit. Descoperirea faptei poate apărea după ce acest „comerciant" a fost deja plătit pentru tranzacţii şi a închis afacerea.
- ***Kiting***: Această formă implică două conturi, folosite pentru scopuri frauduloase: un debit are loc în conexiune cu o tranzacţie din celălalt cont, suma fiind retrasă înainte de finalizarea tranzacţiei. Într-o altă formă, un comerciant îşi poate utiliza cardul de credit în propriul sediu comercial, pentru obţinerea unui rabat[646].
- ***Triangularea***: Această formă se desfăşoară prin intermediul unui site web de tip licitaţie sau vânzare tradiţională, cu o aparenţă de legitimitate, bunurile fiind oferite la preţuri mult scăzute, pentru atragerea clienţilor. Clienţii care plasează comenzi online furnizează nume, adresă şi numere

---

facturi, denumită factor, şi o societate comercială furnizoare de produse sau servicii, denumită aderent. Aderentul urmăreşte să-şi încaseze preţul facturilor înainte de termenul de scadenţă, iar factorul urmăreşte să obţină un beneficiu, de regulă un anumit procent din facturile pe care le decontează în avans. În activitatea de factoring ia parte şi beneficiarul (clientul) care va fi notificat că trebuie să plătească factura la scadenţă factorului. Companiile de factoring se mai ocupă şi de administrarea şi managementul facturilor clienţilor, precum şi de asigurări împotriva riscurilor de neplată a debitorilor.

645 Termenul este folosit în conexiune cu atacuri informatice: direcţionarea datelor către un calculator sau o reţea de calculatoare, astfel încât fluxul mult prea mare de mesaje cauzează o cădere a sistemului.

646 Reducere de preţ acordată de către vânzător cumpărătorului, în cazul de faţă neexistând o vânzare reală de marfă, prin efectuarea tranzacţiei cu cardul de credit se creează în mod fraudulos un plus de numerar pentru comerciant.

BUCHAREST UNIVERSITY LIBRARY

de card; după obţinerea acestora, infractorii comandă bunuri sau servicii de pe site-uri legitime pentru ei[647].

Un alt tip de operaţie frauduloasă similară celei de mai sus este ***frauda funcţionarului instituţiei financiare***. Pentru a crea accesul la informaţiile necesare, grupurile infracţionale au nevoie de oameni în acele locuri unde sunt colectate datele privind cardul şi informaţiile referitoare la posesorul cardului.

Exemple tipice de astfel de locaţii sunt hotelurile, oficiile poştale sau societăţile de curierat, care intră în categoria persoanelor amintite la prezentarea modului de operare „frauda la comerciant", precum şi societăţile care înregistrează plăţile cu cardul. Informaţiile confidenţiale privind conturile ataşate cardurilor sunt divulgate infractorului de către un angajat racolat sau „infiltrat" în compania respectivă, maniera fiind eficientă nu doar pentru copierea informaţiilor de pe benzile magnetice ale cardurilor folosite la plată, ci şi pentru a obţine informaţii personale.

Urmarea imediată constă în starea de pericol la adresa securităţii tranzacţiilor electronice, pentru interesele titularului instrumentului de plată electronică. Infracţiunea prezentată mai sus, alături de celelalte care fac parte din această grupă (Cap. IV), pot produce pagube materiale importante nu numai pentru titularii instrumentelor de plată electronică, ci şi pentru instituţiile emitente.

Textul de lege nu cere, însă, pentru existenţa acestei infracţiuni, să se producă un prejudiciu, astfel că ea va exist,a chiar dacă acesta nu s-a produs. Se aduce, astfel, atingere confidenţialităţii şi încrederii persoanelor în organele care au atribuţii de serviciu privind acceptarea operaţiunilor prevăzute în art. 1, pct. 10 din Legea nr. 365/2002. Rezultatul socialmente periculos rezultă şi din punerea în pericol a protecţiei datelor financiare personale ale părţii vătămate (a se vedea a treia modalitate prezentată).

Legătura de cauzalitate rezultă din simpla comitere a elementului material (*ex re*).

b) **Latura subiectivă** se compune din: elementul subiectiv şi cerinţe esenţiale.

Elementul subiectiv. Infracţiunea se comite cu vinovăţie, în forma intenţiei. Acceptarea operaţiunilor financiare efectuate în mod fraudulos fără a fi cunoscut faptul că sunt efectuate în mod neautorizat şi fraudulos, nu cade sub incidenţa articolului 28, culpa celui vinovat va fi determinata de modul în care au fost prevăzute la nivel intern normele BNR privind răspunderea pentru nerespectarea regulilor privind acceptarea operaţiunilor cu instrumente de plată electronice. Spre exemplu, în conformitate cu prevederile Art. 28 (2) din Regulamentul BNR nr. 6/2006, comerciantul acceptant are obligaţia ca, la momentul prezentării unui instrument de plată electronică pentru efectuarea unei tranzacţii, să verifice, în conformitate cu prevederile contractului încheiat cu instituţia acceptantă şi ale reglementărilor legale, identitatea utilizatorului.

Identitatea utilizatorului se consideră verificată prin introducerea codului PIN sau prin compararea semnăturii de pe chitanţă cu cea existentă pe aversul

[647] Vezi http://achievecard01.blogspot.ro/2013/02/credit-card-fraud-triangulation.html.

instrumentului. Instituțiile acceptante pot stabili, prin prevederile contractuale încheiate cu comercianții acceptanți, în cazul nesolicitării codului PIN de către POS-ul utilizat sau pentru valori ale tranzacțiilor care depășesc o anumită limită, ca identificarea să se facă și prin solicitarea unui act de identitate al deținătorului. În conformitate cu art. 28, comerciantul acceptant are obligația ca, în situația în care, pentru efectuarea unei tranzacții, este obligatorie introducerea de către utilizator a codului PIN, să ia toate măsurile ce se impun pentru asigurarea confidențialității acestei operațiuni.

Prevederi importante în legătură cu forma de vinovăție a acceptantului sunt cuprinse în Regulamentul Băncii Naționale a României nr. 6/2006 privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente, care conține, printre altele, prevederi speciale referitoare la identificarea fraudelor cu carduri. Astfel, în capitolul III – Emiterea instrumentelor de plată electronică și identificarea fraudelor, Secțiunea a II-a – Fraude și activități cu risc potențial, art. 37 stipulează: În cadrul procesului de monitorizare a tranzacțiilor cu carduri efectuate la comercianții acceptanți, băncile acceptante[648] au obligația de a identifica activitatea frauduloasă. Acestea vor identifica cel puțin următoarele tipuri de fraudă:

- Acceptarea repetată la plată, cu intenție sau din culpă, de carduri contrafăcute;
- Furnizarea către persoane neautorizate de informații cu privire la carduri valide acceptate la plată (prin copierea benzii magnetice sau a informațiilor embosate ori gravate pe suprafața cardului și transmiterea acestor date către acestea);
- Dublarea de către comerciantul acceptant a chitanțelor aferente unor tranzacții și remiterea acestora spre încasare băncii acceptante.

Potrivit art. 38 din același Regulament, emitentul[649] are obligația să identifice activitatea frauduloasă, să se informeze în legătură cu aceasta din orice sursă, pentru evitarea riscurilor de neplată, și să ia toate măsurile ce se impun pentru limitarea fraudelor și descurajarea tentativelor de fraudă. În investigațiile sale privind activitatea frauduloasă, emitentul va analiza inclusiv următoarele situații:

- Utilizarea unui card pierdut - utilizatorul cardului contestă, în mod legitim, o tranzacție efectuată pe contul sau ulterior pierderii reclamate de către acesta;
- Furtul cardului - utilizatorul cardului contestă, în mod legitim, o tranzacție efectuată pe contul sau ulterior furtului reclamat de către acesta;

---

648 Banca acceptantă oferă comercianților servicii de acceptare la plată a cardurilor și/sau a instrumentelor de plată tip monedă electronică (*e-money*), în baza unui contract încheiat în prealabil între bancă și comerciant, precum și servicii de eliberare de numerar la ghișeele băncii și în rețeaua proprie de automate bancare.

649 Emitentul este o bancă autorizată de Banca Națională a României să emită instrumente de plată electronică și care pune la dispoziție deținătorului un instrument de plată electronică, pe baza unui contract încheiat cu acesta.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

- Emiterea şi nerecepţionarea cardului de către utilizator - utilizatorul cardului contestă, în mod legitim, o tranzacţie efectuată pe contul său, ca urmare a faptului că acesta reclamă nerecepţionarea cardului emis pe numele său şi emitentul confirmă că a transmis cardul utilizatorului;
- Cerere de eliberare a cardului eronată sau completată fraudulos - deţinătorul cardului contestă, în mod legitim, o tranzacţie efectuată pe contul său, ca urmare a faptului ca acesta susţine că nu a solicitat niciodată emiterea unui card pe numele său sau emitentul confirmă că informaţiile privind deţinătorul cardului au fost introduse în mod eronat pe formularul de cerere de emitere a cardului;
- Utilizarea în cadrul tranzacţiilor a unui card contrafăcut - deţinătorul cardului contestă, în mod legitim, o tranzacţie efectuată pe contul său, ca urmare a faptului că acesta reclamă neautorizarea tranzacţiei de către deţinător, iar emitentul confirmă ca banda magnetică şi/sau cardul au fost copiate şi informaţiile au fost folosite pentru efectuarea tranzacţiei;
- Folosirea frauduloasă a cardului de către o persoană neautorizată - deţinătorul cardului contestă, în mod legitim, o tranzacţie efectuată pe contul său, ca urmare a faptului că acesta reclamă neautorizarea tranzacţiei de către utilizator, iar emitentul confirmă că o altă persoană s-a prezentat, în mod fraudulos, ca utilizator al cardului;
- Folosirea frauduloasă a numărului de cont al cardului în cadrul unei tranzacţii - utilizatorul cardului contestă, în mod legitim, o tranzacţie efectuată pe contul său, ca urmare a faptului că acesta reclamă că tranzacţia nu a fost autorizată de către utilizator, iar numărul său de cont a fost folosit în mod ilegal într-o tranzacţie ce nu necesită prezenţa fizică a cardului (tranzacţii efectuate prin Internet sau telefon);
- Frauda identificată de instituţia acceptantă la comerciantul acceptant - deţinătorul cardului contestă, în mod legitim, o tranzacţie efectuată pe contul său şi instituţia acceptantă confirmă emitentului că tranzacţia respectivă a avut loc ca urmare a unei fraude la comerciantul acceptant, prin duplicarea chitanţei aferente unei tranzacţii, autorizată sau neautorizată, şi transmise acestuia pentru plată.

De asemenea, Regulamentul prevede obligativitatea pentru emitent şi banca acceptantă de a-şi organiza activitatea de evidenţă a informaţiilor şi datelor obţinute privind tranzacţiile efectuate prin intermediul cardurilor, astfel încât să permită oricând realizarea unor situaţii şi raportări solicitate de autorităţile competente în domeniu. Reglementările prezintă un interes practic deosebit având în vedere posibilitatea procurorilor Direcţiei de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism de a dispune să li se comunice înscrisuri, documente bancare, financiare ori contabile sau punerea sub supraveghere a conturilor bancare şi a conturilor asimilate acestora în scopul strângerii de probe şi

sau al identificării făptuitorului, potrivit Legii nr. 508/2004[650] şi a dispoziţiilor Codului de procedură penală.

Mobilul şi scopul vor fi luate în considerare la individualizarea judiciara a pedepsei.

Forme. Modalităţi. Sancţiuni

A. Forme

a) Actele de pregătire sunt posibile, dar incriminarea lor nu este prevăzută de acest text de lege.

b) Tentativa. *Actele de executare* (*tentativa*) sunt posibile şi pedepsite în conformitate cu prevederile art. 252.

c) Consumarea infracţiunii are loc în momentul acceptării de către subiectul activ a efectuării operaţiunii frauduloase.

d) Epuizarea. Acţiunile de acceptarea a operaţiunilor financiare efectuate în mod fraudulos pot îmbrăca, uneori, şi forma unei activităţi continuate, iar în acest caz poate avea şi o formă epuizată, care este ultimul act de acceptare a unei operaţii frauduloase.

B. Modalităţi

a) Modalităţile normative simple. În raport cu elementul normativ al infracţiunii de acceptarea a operaţiunilor frauduloase efectuate în mod fraudulos există trei modalităţi normative şi anume:

- Acceptarea unei operaţiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, cunoscând că este efectuată prin folosirea unui instrument de plată electronică falsificat;
- Acceptarea unei operaţiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, cunoscând că este efectuată prin folosirea unui instrument de plată electronică, utilizat fără consimţământul titularului său,
- Acceptarea unei operaţiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, cunoscând că este efectuată prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.

b) Modalităţi de fapt. Acceptarea de operaţiuni financiare efectuate în mod fraudulos prezintă numeroase şi variate posibilităţi de realizare, cu particularităţi care duc, în mod firesc, la existenţa unui bogat cadru de comitere a infracţiunii. Particularităţile care diferenţiază aceste modalităţi privesc elementele structurale ale infracţiunii sau alte aspecte. Facem trimitere la analiza elementului material al laturii obiective unde am prezentat cele mai frecvente modalităţi de fapt sub care se pot prezenta modalităţile normative.

---

[650] Privind înfiinţarea, organizarea şi funcţionarea, în cadrul Ministerului Public, a Direcţiei de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism (M. Of. nr. 1089 din 17 noiembrie 2004).

C. Sancțiuni

Pedeapsa prevăzută pentru acceptarea operațiunilor financiare efectuate în mod fraudulos este închisoare de la unu la 5 ani (în cazul tentativei, limitele pedepsei se reduc la jumătate). Din păcate, legiuitorul penal nu a dorit să țină seama de semnalele multiple, atât la nivelul Uniunii Europene, cât și la nivel global, în legătură cu înăsprirea pedepselor pentru acest tip de fraude, care distrug încrederea consumatorilor în plățile electronice și produc pagube materiale foarte mari. În loc să facă acest lucru, legiuitorul a redus pedeapsa prevăzută de Legea nr. 365/2002 (închisoare de la unu la 12 ani), rezultatul fiind unul dintre cele mai blânde tratamente penale aplicate făptuitorilor de acest tip.

Aspecte procesuale: Acțiunea penală se pune în mișcare din oficiu. Competența de judecată în primă instanță este judecătoria.

Precedente legislative

Așa cum am menționat la începutul analizei acestei infracțiuni, ea a fost pentru prima dată prevăzută în Legea Comerțului electronic (la art. 28).

Elemente de drept comparat

Având în vedere faptul că, în ceea ce privește comerțul electronic și mijloacele de plată electronice, există un complex cadru legal european (a se vedea explicațiile date în cadrul analizei), cu obligații pentru statele membre de a adopta măsuri penale de protecție a relațiilor în acest domeniu, există reglementări similare în toate statele membre ale UE, iar datorită expunerii globale a tranzacțiilor electronice, în numeroase state la nivel mondial.

4.5 Falsul informatic

Art. 325. Fapta de a introduce, modifica sau șterge, fără drept, date informatice ori de a restricționa, fără drept, accesul la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice, constituie infracțiune și se pedepsește cu închisoarea de la unu la 5 ani.

Conținut legal și caracterizare

Scopul prevederii acestui articol în legislațiile penale a fost de a crea o variantă de specie, în paralel cu infracțiunea de fals ce privește documentele materiale (tangibile). Majoritatea legislațiilor penale în materie de fals prevăd ca afirmațiile sau declarațiile ce figurează într-un document să poată fi descifrate cu ochiul liber, astfel încât ele nu se aplică datelor informatice, ceea ce prezintă serioase lacune în domeniul digital[651]. Manipulările de date informatice, având

[651] În unele țări, manipulările frauduloase în această materie au fost acoperite de dispozițiile referitoare la falsificarea de documente (spre exemplu, în Norvegia, Elveția etc.). Totuși, în cea mai mare parte a țărilor, dispozițiile penale în materie de fals cer ca afirmațiile sau declarațiile

BCU IAȘI CENTRAL UNIVERSITY LIBRARY

forţă probatoare, duc la aceleaşi consecinţe grave ca actele tradiţionale de contrafacere dacă, spre exemplu, acestea induc în eroare un terţ şi ar fi inadmisibil ca asemenea date să scape protecţiei penale în materie de contrafacere.

Scopul textului propus de Convenţia europeană în domeniul criminalităţii informatice[652] este, prin urmare, acela de a acoperi lacunele dreptului penal privind falsul tradiţional şi care cere, ca o condiţie esenţială, ca declaraţiile sau afirmaţiile ce figurează într-un document să poată fi descifrate cu ochiul liber, condiţie ce nu poate fi îndeplinită în cazul datelor informatice stocate pe suporturi magnetice.

Textul art. 325 din noul Cod penal reproduce art. 48 al Legii nr. 161/2003, articol similar celui propus de Convenţia europeană în domeniul criminalităţii informatice, pedepseşte ca "fals informatic", adică fapta de a introduce, modifica sau şterge, fără drept, date informatice, ori de a restricţiona, fără drept, accesul la aceste date, dacă fapta are ca rezultat obţinerea de date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii de consecinţe juridice. Singura diferenţă din art. 325 a noului Cod penal este cea privitoare la sancţiune, care a fost redusă, pentru a o corela cu restul pedepselor din grupa de infracţiuni „Falsul în înscrisuri" în care a fost inclusă.

Importanţa deosebită care se acordă actualmente la nivel global protecţiei prin mijloace penale împotriva activităţilor de falsificare în mediul electronic prin conştientizarea periculozităţii acestor fapte este arătată şi prin propunerea acestei infracţiuni de fals informatic (în forma consacrată de Convenţia europeană privind criminalitatea informatică şi preluată de legislaţia penală românească) în propunerea Naţiunilor Unite de *Tratat Global în domeniul securităţii şi criminalităţii informatice* din 2010[653].

Elemente preexistente

Obiectul infracţiunii

Obiectul juridic al infracţiunii este reprezentat de aceleaşi valori care sunt protejate în dreptul tradiţional în materie de fals: securitatea şi fiabilitatea documentelor sau altor instrumente care pot avea consecinţe juridice. A fost lărgit numai cadrul intereselor, beneficiindu-se de această protecţie atunci când documentele sau instrumentele supuse acţiunii de contrafacere în scopul obţinerii consecinţelor juridice dorite de făptuitor conţin sau privesc date informatice.

Obiectul juridic special al acestei infracţiuni îl formează, în consecinţă, relaţiile sociale a căror formare şi desfăşurare normală şi a căror dezvoltare depinde de încrederea publică acordată *înscrisurilor electronice*.

Obiectul material al infracţiunii îl constituie suportul material pe care sunt înscrise sau stocate datele informatice supuse ingerinţei făptuitorului sau părţile

---

ce figurează într-un document să poată fi descifrate cu ochiul liber.

652 Acest text este foarte apropiat de cel din Recomandarea R (89)9 a Comitetului European pentru Probleme Criminale.

653 A se vedea, art. 7, Falsul informatic (*Computer-related forgery*), în *Draft code on peace, justice and security in cyberspace - A global traty on cybersecurity and cybercrime* (noiembrie 2010); pentru amănunte referitoare la acest tratat, a se vedea http://www.itu.int/osg/csd /cybersecurity/gca/global_strategic_report/index.html.

BCU IASI CENTRAL UNIVERSITY LIBRARY

sistemului informatic asupra cărora se acţionează pentru a restricţiona accesul la date informatice.

Subiecţii infracţiunii

a) Subiect activ al infracţiunii poate fi orice persoană fizică sau juridică, textul nefăcând nici o referire la vreo calitate specială pe care trebuie să o îndeplinească autorul (facem precizarea că, cel mai adesea, manipulările de tipul falsului informatic sunt efectuate de persoane ce au cunoştinţe de specialitate în acest domeniu sau au acces la sisteme informatice).

Participaţia penală este posibilă sub toate formele: instigare, complicitate sau coautorat.

b) Subiect pasiv al infracţiunii este persoana fizică sau juridică în contra căreia ingerinţa de tipul falsului informatic produce consecinţe juridice (persoana căreia i se atribuie documentul sau înscrisul electronic).

Structura juridică şi Conţinutul constitutiv a infracţiunii

Latura obiectivă

Elementul material se realizează prin una din următoarele acţiuni: introducerea, modificarea, ştergerea de date informatice sau restricţionarea accesului la date informatice, cu condiţia ca acestea să fie realizate *fără drept*.

Introducerea de date informatice se referă la tastare sau inserare prin alte modalităţi (spre exemplu, prin folosirea unui modem, scanner sau diverse tipuri de discuri) de date într-un sistem informatic[654]. *Modificarea* datelor informatice se referă la orice alterare a acestora, schimbare sau variaţie în conţinutul lor (adesea prin folosirea de contaminanţi informatici). *Ştergerea* constituie fapta de a elimina datele stocate pe un suport fizic.

Restricţionarea accesului la date informatice se referă la fapta de a preveni accesul la date, a le plasa în locaţii unde sunt greu de găsit sau accesat sau întârzierea semnificativă a accesului la aceste date, ceea ce are ca rezultat blocarea accesului la date atunci când este nevoie de ele pentru ca o operaţie informatică să se desfăşoare corect şi complet. În practică, realizarea restricţionării accesului la date informatice se realizează destul de frecvent prin atacuri de tip *Denial of Service* (refuzul serviciului). Modalităţile de comitere în practică ale acestei infracţiuni, datorită sofisticării domeniului tehnologiei informaţiei şi comunicaţiilor şi inventivităţii făptuitorilor, sunt foarte variate.

Un tip de fals informatic frecvent întâlnit este alterarea link-ului, tip de falsificare cunoscut şi sub numele de "Web forgery" sau *phishing*. Acesta reprezintă un furt de identitate, care are loc când un site web creat de un hacker impersonează pe cel legitim, pentru a induce în eroare utilizatorii şi a obţine informaţii senzitive, cum ar fi parole sau detalii privind numere de carduri bancare sau conturi. Atacurile de acest tip se comit, de regulă, prin utilizarea mesajelor de poştă electronică, dar şi prin mesaje pe telefoanele mobile de ultimă generaţie (de

---

[654] În legătură cu descrierea acestor dispozitive, vezi I. Vasiu şi L. Vasiu, *Informatică juridică şi Drept informatic 2009*, op. cit.

unde şi denumirea acestei metode "smishing"), încercând sa-i atragă pe recipienţi să introducă date personale pe aceste site-uri web false[655].

Toate acţiunile descrise de legiuitor prin care se ajunge la o situaţie ce corespunde fabricării unui document electronic fals, pentru a face obiectul laturii obiective a infracţiunii, trebuie realizate fără drept, adică fără autorizarea proprietarului sau utilizatorului datelor sau sistemului informatic şi cu încălcarea reglementărilor legale în materie.

Urmarea imediată. Pentru existenţa laturii obiective, este necesar ca acţiunea de falsificare - realizată prin introducerea, modificarea sau ştergerea de date informatice sau prin restricţionarea accesului la date informatice - să aibă ca urmare imediată crearea unei stări de pericol pentru relaţiile sociale ocrotite, pericol decurgând din realizarea unui înscris electronic fals ce prezintă toate însuşirile unui înscris electronic corespunzător.

Legătura de cauzalitate. Pentru ca starea de pericol să fie considerată produs al unei acţiuni de falsificare, trebuie să se constate că între starea de pericol şi acţiunea realizată prin modalităţile arătate există o legătură de cauzalitate.

Latura subiectivă

Fapta prevăzută de legiuitor în art. 325 va constitui infracţiunea de fals informatic numai dacă a fost săvârşită cu forma de vinovăţie *intenţia* şi în *scopul* de a utiliza datele necorespunzatoare adevărului în vederea producerii de consecinţe juridice. Cerinţa legată de acest scop este îndeplinită din momentul în care înscrisul falsificat are aparenţa însuşirilor unui înscris electronic adevărat şi ar putea, prin folosire, produce aceleaşi efecte ca acesta din urmă.

Formele infracţiunii

a) Actele pregătitoare, deşi sunt posibile şi uneori necesare, nu cad sub incidenţa acestui text (ele pot face obiectul infracţiunii din art. 365 noul Cod penal).

b) Tentativa este posibilă, dar potrivit noului Cod penal nu mai este pedepsită (nemai preluându-se prevederea din art. 50 al Legii nr. 161/2003, potrivit căreia aceasta era pedepsită).

Consumarea infracţiunii are loc în momentul producerii urmării imediate, adică obţinerea de date necorespunzătoare adevărului, creându-se, astfel, starea de pericol pentru relaţiile sociale ocrotite.

Epuizarea infracţiunii are loc în momentul comiterii ultimului act incriminat de textul art. 325. Infracţiunea este susceptibilă de a fi comisă în forma continuată.

Sancţiunea

Falsul informatic se pedepseşte cu închisoare de la unu la 5 ani. Din păcate, după cum se poate observa din comparaţia pedepselor din noul Cod penal şi din Legea nr. 161/2003, legiuitorul noului Cod penal, a redus pedeapsa în cazul acestei

---

[655] Vezi, pentru amănunte, http://www.antiphishing.org/.

infracţiuni, de la 2 la 7 ani, în conformitate cu prevederile art. 48 din Legea nr. 161/2003 la închisoare de la unu la 5 ani.

4.6 Infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice

4.6.1 Introducere

Concept şi caracterizare

După cum se subliniază în Directiva 2013/40/UE a Parlamentului european şi a Consiliului, sistemele informatice reprezintă un element fundamental al interacţiunii sociale şi economice, dependenţa de aceste sisteme fiind în creştere. Atacurile contra siguranţei şi integrităţii sistemelor şi datelor informatice sunt în creştere în ultimii ani, atât în ceea ce proveşte numărul, cât şi sofistacarea lor. Conform Directivei COM(2013) 48 privind măsuri de asigurare a unui nivel comun ridicat de securitate a reţelelor şi a informaţiei în Uniune, 57 % dintre respondenţii la consultarea Comisiei Europene privind „Îmbunătăţirea securităţii reţelelor şi a informaţiei în UE" au afirmat că "s-au confruntat în anul precedent cu incidente de securitate a reţelelor şi a informaţiei care le-au afectat grav activitatea". Securitatea acestor sisteme este vitală pentru dezvoltarea economică, motiv pentru care au fost introduse dispoziţii penale privind atacurile împotriva securităţii datelor şi sistemelor informatice.

Pe măsură ce societatea contemporană devine hiper-conectată, creşte şi prevalenţa criminalităţii informatice. Nici un stat nu poate de unul singur să elimine sau măcar să reducă problema infracţionalităţii în cyberspaţiu. Este nevoie de leadership partajat şi determinare, un demers în acest sens fiind reprezentat de Convenţia europeană (ETS No. 185), considerată un început pozitiv, dar care, mai ales în contextul evoluţiilor foarte dinamice din domeniul tehnologiilor informaţiei şi comunicaţiei, trebuie continuat şi îmbunătăţit în ceea ce priveşte detalierea elementelor necesare în cazul fiecărei infracţiuni, specificarea unor proceduri consistente[656].

Criminalitatea în cyberspaţiu a crescut în sofisticare şi prevalenţă[657], implicând, din ce în ce mai mult, crima organizată, hacking-ul, utilizarea botnet-

---

[656] Imperfecţiunile Convenţiei europene în domeniu şi discuţiile de adaptare a acesteia la nevoile prezentului în lupta împotriva criminalităţii informatice sau de adoptare a unui alt mecanism global în domeniu, s-au concretizat într-o serie de iniţiative, cum ar fi ITU Toolkit, disponibil la http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html; a se vedea şi studiul lui Michael A. Vatis, *The Council of Europe Convention on Cybercrime*, Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy, disponibil la http://www.nap.edu/catalog/12997.html.

[657] Vezi, spre exemplu, Verizon, *Data Breaches Investigations Report*, 2013; Sophos, *Security Threat Report*, 2013.

BCU IASI CENTRAL UNIVERSITY LIBRARY

urilor, furtul de date din interiorul organizațiilor și atacuri coordonate masive asupra infrastructurilor de informații critice, pagubele înregistrate datorită acestui tip de criminalitate fiind în continuă creștere. Această situație îngrijorează organizațiile în mod deosebit, ajungându-se la ideea de a lansa sateliți în spațiu, cu scopul de a crea un backup al tranzacțiilor[658].

Atacurile informatice ridică probleme noi și multiple și pot afecta toate nivelele societății. Atacurile informatice vizează și afectează persoane fizice din toate grupurile demografice (bărbații și femeile raportând crime într-o proporție aproape egală[659]), firme mici și mijlocii (IMM-uri[660]), instanțe de judecată[661], operatori bursieri[662], corporații globale[663], organisme guvernamentale, întregi industrii[664] sau chiar țări (vezi, spre exemplu, cazul atacului informatic asupra Estoniei)[665].

Impactul atacurilor informatice, depinde de victimă și alte circumstanțe, dar poate consta în pagube financiare mari, încălcarea drepturilor de proprietate intelectuală, contaminarea sau copierea datelor informatice, blocarea accesului la date informatice, repudierea tranzacțiilor sau comunicațiilor electronice, încetinirea vitezei de procesare a datelor ș.a.[666] Pentru aceste motive, securitatea cyberspațiului (*cybersecurity*), armonizarea legislației și cooperarea internațională

---

[658] Vezi *Bitcoin se pregatește sa ajungă și în spațiu*, 2014, disponibil la https://ro.stiri.yahoo.com /bitcoin-se-preg%C4%83te%C8%99te-s%C4%83-ajung%C4%83-%C8%99i-%C3%AEn -spa%C8%9Biu-080956164.html.

[659] Vezi Internet Crime Complaint Center, *2010 Internet Crime Report*, 2011.

[660] Vezi, spre exemplu, cazul raportat în anul 2010 de Wall Street Journal, în care o rețea internațional de criminali a furat circa 70 milioane dolari de la mici firme, municipalități și biserici, raportat în Verisign, *The domain name industry brief*, Vol. 8, Iss. 3, August, 2011.

[661] Contaminantul informatic Downadup a afectat rețeaua de calculatoare a Penitenciarului Rahova, rețeaua interna a IGPR și rețeaua Tribunalului București, rezultând în nefuncționarea sistemului ECRIS (sistemul informatic de management al dosarelor de judecată) – vezi detalii la http://www.mondonews.ro/Virusul-Downadup-a-atacat-mai-multe-institutii+id-7424.html. Sistemul municipal de justiție din Houston, Texas a fost infectat de contaminanți informatici, rezultând în afectarea capacității de acțiune a poliției – vezi detalii la http://www.chron .com/disp/story.mpl /front/6250411.html.

[662] D. Barrett, *Hackers Penetrate Nasdaq Computers*, Wall Street Journal, February 5, 2011.

[663] Cazul Aurora, spre exemplu: în ianuarie 2010, un atac informatic asupra mai multor corporații globale, printre care Google, IBM, Microsoft și Adobe, declanșat din China – vezi detalii în A. Boulanger și S. Ghosh, *Malicious Code*, În S. Ghosh și E. Turrini (eds.), *Cybercrimes: A Multidisciplinary Analysis*, 2010; Symantec, *Global Internet Security Threat Report Trends for 2009*, Vol. XV, April, 2010. Vezi și cazurile Sony, Honda, Fox News, Epsilon și Citibank, menționate în Kaspersky Lab, *IT Threat Evolution: Q2 2011*, 2011.

[664] Vezi McAfee, *Global Energy Cyberattacks: "Night Dragon"*, February 10, 2011.

[665] Descris în M. Donner, *Cyberassault on Estonia*, IEEE Security & Privacy, Vol. 5, Iss. 4, 2007, p. 4; vezi și G. Evron, *Battling botnets and online mobs: Estonia's defense efforts during the Internet war*, Georgetown Journal of International Affairs, 9(1), 121–126, 2008.

[666] Vezi numeroase studii pe această temă: Verizon, *Data Breach Investigations Report*, 2014; JP Morgan Chase, *Cybercrime: The Growing Global Threat*, 2011; Uniunea Eurpeană, http://ec.europa.eu/home-affairs/policies/crime/crime _cybercrime _en.htm (circa 750 miliarde euro anual); PricewaterhouseCoopers, *Global State of Information Security Survey*, 2011; Ernst & Young, *Insights on IT Risk*, April, 2011; Interpol, *Financial and High-tech Crimes*, 2009; United Nations Conference on Trade and Development, *Information Economy Report*, 2005.

în acest domeniu sunt foarte importante, fapt reflectat, printre altele, de numeroase inițiative legislative[667], Rezoluții ale Națiunilor Unite[668] sau Uniunea Internațională a Telecomunicațiilor (ITU, agenție a Națiunilor Unite)[669] sau conferințe internaționale pe această temă[670].

Acest capitol de infracțiuni contra siguranței și integrității sistemelor și datelor informatice nu are corespondent în vechiul Cod penal, grupa și infracțiunile componente fiind în totalitate preluate (cu mici modificări de sistematizare, respectiv schimbări nesemnificative de termeni-cheie) din Legea nr. 161/2003, a cărei sursă este Convenția europeană privind criminalitatea informatică. Prevederea în noul Cod penal a infracțiunilor posibile sau facilitate de noile tehnologii ale informației și comunicațiilor, în special a infracțiunilor contra siguranței și integrității sistemelor și datelor informatice, constituie o acțiune necesară de armonizare a legislației noastre penale la cel mai înalt nivel cu legislația europeană și globală în domeniu, precum și reacția necesară la creșterea exponențială a acestui tip de infracționalitate[671].

În România, conform Ordonanței de Guvern Nr. 1040/2010, prevenirea și combaterea criminalității informatice este obiectiv strategic. Importanța luptei împotriva acestui tip de criminalitate este subliniată și în Hotărârea Guvernului nr. 271/2013, pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică[672]. Legea privind Securitatea Cibernetică a României, adoptată de Guvern în 30 aprilie 2014, impune deținătorilor de infrastructuri cibernetice să implementeze măsuri tehnice și organizatorice pentru gestionarea efectivă a riscurilor de securitate.

În noul Cod penal, legiuitorul a prevăzut grupa de infracțiuni contra confidențialității, integrității și disponibilității datelor și sistemelor informatice (în mod incomplet și oarecum redundant numită de legiuitorul nostru penal "Infracțiuni contra siguranței și integrității sistemelor și datelor informatice") la Cap. VI al Titlului VII "Infracțiuni contra siguranței publice". Capitolul cuprinde șase infracțiuni: accesul ilegal la un sistem informatic, interceptia ilegală a unei

---

667 Vezi, spre exemplu, The White House, Office of the Press Secretary, *Cybersecurity Legislative Proposal*, May 12, 2011.

668 A se vedea Rezoluțiile 22/8 - *Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime*; 56/121 - *Combating the criminal misuse of information technologies* (2002) și 55/63 - *Combating the criminal misuse of information technologies* (2001).

669 Vezi, spre exemplu, Rezoluția 181 (Guadalajara, 2010) - *Definitions and terminology relating to building confidence and security in the use of information and communication technologies* și Rezoluția 130 - *Strengthening the role of ITU in building confidence and security in the use of information and communication technologies*.

670 Vezi, spre exemplu, J. Vogel, *Towards a Global Convention against Cybercrime*, First World Conference of Penal Law. Penal Law in the XXIst century, Guadalajara, Mexic, 2007.

671 Vezi Federal Bureau of Investigations (FBI), *Facts and Figures 2013-2014*; Kaspersky Lab, *More users, more attacks: Kaspersky Lab stats show a surge in Bitcoin cybercrime*, 2014; Ben Dipietro, *Cybercrime 2014: More Attacks, More Boardroom Scrutiny*, Wall Street Journal, December 3, 2013.

672 Publicată în Monitorul Oficial, Partea I, Nr. 296, 23.05.2013.

BCU IAȘI CENTRAL UNIVERSITY LIBRARY

transmisii de date informatice, alterarea integrității datelor informatice, transferul neautorizat de date informatice, perturbarea funcționării sistemelor informatice și operațiuni ilegale cu dispozitive sau programe informatice.

Legiuitorul noului Cod penal schimbă ușor, probabil din neatenție, titlul grupei (preluat corect din Convenția europeană privind criminalitatea informatică în legea de ratificare a acesteia din anul 2004, adică "*Infracțiuni contra confidențialității integrității și disponibilității sistemelor și datelor informatice*"), acesta fiind, cum am menționat mai sus, în noul Cod penal "Infracțiuni contra siguranței și integrității sistemelor și datelor și sistemelor informatice", omițând două concepte/elemente cheie ale securității informatice. Infracțiunile sunt preluate, fără modificări semnificative, din Legea nr. 161/2003. Modificările privesc, în principal, regimul sancționatoriu, legiuitorul noului Cod penal, propunând pedepse mai mici decât cele din Legea nr. 161/2003.

De remarcat că legiuitorul a preluat chiar și în Legea nr. 161/2003 (principala sursă de inspirație pentru noul Cod penal) numai parțial titlul subgrupei din Convenția europeană, omițând un concept/element cheie: disponibilitatea datelor și sistemelor informatice – vezi Convenția privind criminalitatea informatică, Titlul 1: *Offences against the confidentiality, integrity and availability of computer data and systems* (*Infracțiuni contra confidențialității integrității și disponibilității sistemelor și datelor informatice)*. De altfel, și în Codul penal adoptat prin Legea nr. 301/2004, a cărui intrare în vigoare a fost amânată succesiv, până la abrogarea sa prin art. 446 alin. 2 din Legea nr. 286/2009, legiuitorul nostru a ales un titlu incomplet pentru acest capitol, și anume: Cap. I "Delicte contra confidențialității și integrității datelor și sistemelor informatice" (Titlul X Delicte contra datelor și sistemelor informatice).

Chiar dacă în Convenție se precizează că în dreptul național nu este necesar să apară *verbatim* conținutul acesteia, considerăm că omisiuni și imprecizii de acest tip pot duce la interpretări sau aplicări greșite sau incomplete ale prevederilor legale în practică.

Elemente preexistente

A. Obiectul juridic generic sau de grup al infracțiunilor din acest capitol îl constituie relațiile sociale a căror naștere și dezvoltare este condiționată de siguranța și integritatea sistemelor informatice, sau cum mai exact precizează legiuitorul european în Convenția privind criminalitatea informatică: confidențialitatea, integritatea și disponibilitatea datelor și sistemelor informatice. Aceste elemente fundamentale ale securității sistemelor și datelor informatice apar și în propunerea de Tratat global privind securitatea și criminalitatea informatică[673].

Cerințele de securitate ale sistemelor informatice, foarte complexe, au la bază numeroase aspecte operaționale, economice, tehnice, politice, legale, societale și umane; dintre acestea, lupta împotriva criminalității informatice

---

673 Vezi pentru detalii, Ioana Vasiu, Lucian Vasiu, *Criminalitatea în cyberspațiu*, op. cit., p. 121-138.

reprezintă un element fundamental[674]. Conform multor autori[675], securitatea în domeniul sistemelor informatice se referă, în primul rând, la *confidențialitate, integritate* și *disponibilitate*.

B. Obiectul material constă de regulă în entitățile materiale care reprezintă sistemele informatice sau cele pe care sunt stocate datele informatice sau informațiile.

C. Subiecții infracțiunii

a) **Subiect activ** poate fi orice persoană (fizică sau juridică) care are capacitate penală, textul de lege neprevăzând la nici una din infracțiunile acestui capitol vreo calitate specială pentru acesta. De regulă, însă, autorul este o persoană care are aptitudini sau cunoștințe tehnice în domeniul calculatoarelor, o anumită familiaritate cu sistemele de securitate informatică și vulnerabilitățile acestor sisteme sau persoane care sunt angajați ai entităților deținatoare ale sistemelor informatice (utilizatori de orice tip, care depășesc nivelul de acces permis).

Participația penală este posibilă sub toate formele: coautorat, complicitate sau instigare.

b) **Subiect pasiv** al infracțiunilor din acest capitol este persoana fizică sau juridică ce are în proprietate sistemele informatice și al cărui drept la integritatea, confidențialitatea și/sau disponibilitatea sistemelor și/sau datelor informatice a fost încălcat sau periclitat.

Structura și conținutul juridic al infracțiunii

Aceasta este alcătuită dintr-o **situație premisă** și un **conținut constitutiv** al infracțiunii.

A. Situația premisă. Aceste infracțiuni nu pot exista în absența unui **sistem informatic** și/sau a unor **date informatice** asupra cărora făptuitorul să acționeze fără drept, neautorizat sau depășind autorizarea, în modalitățile prevăzute pentru realizarea scopului prevăzut în textele de lege. La anumite infracțiuni, numai o componentă, sau anumite componente ale sistemului informatic (dispozitive, programe informatice, coduri de acces, parole, proceduri) constituie situația premisă a acelei infracțiuni contra securității sistemelor informatice.

Necesitatea unei definiții legale cât mai precise a acestui concept-cheie a fost invocată de nenumărate ori la nivel național și internațional. În țările care nu au o definiție legală a sistemului informatic (spre exemplu, Italia sau Australia), s-au întâmpinat unele dificultăți în a determina care tipuri de sisteme informatice pot fi incluse sau nu în această categorie în diferitele situații din practică (spre exemplu, dispozitivele mobile, de genul tablete, smart phone, prin care se realizează accesul

---

[674] Vezi Comunicarea Comisiei Europene, *Către o politică generală de luptă împotriva criminalității cibernetice*, COM(2007) 267 final; vezi și D. B. Hollis, *An e-SOS for Cyberspace*, Harvard International Law Journal, Vol. 52, No. 2, Summer, 2011.

[675] Vezi, spre exemplu, D. L. Pipkin, *Information security: Protecting the global enterprise*, Prentice Hall, 2000; C. P. Pfleeger, *Security in Computing*, Addison Wesley, 1997; P. G. Neumann, *Computer related risks*, ACM Press, 1995.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

la Internet, precum și alte dispozitive optice, electromagnetice sau de înaltă viteză pentru procesarea datelor informatice). În alte țări, cum este România, nu lipsa definiției legale, ci interpretarea ei defectuoasă în cazurile din practică a dus la soluții diferite sau defectuoase date de instanțele de judecată, în situații similare, care au condus la promovarea și acceptarea în 14 octombrie 2013 a unui Recurs în Interesul Legii[676].

Soluțiile recomandate de către instanța supremă pentru definirea unor termeni-cheie (cum ar fi "sistem informatic" sau "acces la un sistem informatic"), respectiv interpretarea situațiilor de fapt și realizarea încadrărilor juridice își mențin valabilitatea și după intrarea în vigoare a noului Cod penal (1 februarie 2014) și abrogarea prevederilor speciale din Legea nr. 161/2003 și Legea nr. 365/2002, urmând a fi aplicabile articolele corespunzătoare din noul Cod penal. Noul Cod penal, în art. 181 (alin. 1 și alin. 2), a preluat definițiile legale ale termenilor-cheie *sistem informatic* și *date informatice*, utilizate de legiuitor în cadrul capitolului de față, din Convenția europeană privind criminalitatea informatică[677].

Conținutul constitutiv al infracțiunii

a) Latura obiectivă

Elementul material al acestor infracțiuni se realizează de regulă prin acțiuni de accesare, intercepție, ștergere, deteriorare, restricționare ilegală a datelor sau sistemelor informatice. Aceste acțiuni se săvârșesc adesea cu ajutorul unor instrumente numite generic *malware* (programe malițioase sau contaminanți informatice). De altfel, operațiunile ilegale cu astfel de dispozitive sunt încriminate separat în acest capitol.

Actualmente există o mare varietate de forme de *malware*. Termenul de *malware* a fost definit de OECD ca fiind "un termen general pentru a desemna un program de calculator (*software*) inserat într-un sistem informatic pentru a cauza un rău acelui sistem sau altor sisteme, sau pentru a prelua controlul asupra acestuia (acestora) și a-l utiliza în alte scopuri decât a intenționat deținătorul legitim"[678]. Cele mai cunoscute forme de *malware* includ viermii, virușii și caii troieni.

Numărul și varietatea formelor de programelor informatice malițioase (*malware*) sunt atât de multe încât este dificil a le prezenta în detaliu[679]. De altfel, Convenția europeană împotriva criminalității informatice or alte acte normative în domeniu, în mod deliberat nu utilizează termeni ca *viermi, viruși sau cai troieni informatici*. Datorită faptului că "tendința" în domeniul programelor malițioase (*malware*) se schimbă rapid, utilizarea unor asemenea termeni ar putea duce repede la lipsa de eficacitate a unor asemenea prevederi sau ar putea deveni chiar contraproductive. În opinia noastră, focalizarea legiuitorului trebuie să fie pe

---

676 A se vedea Înalta Curte de Casație și Justiție – ÎCCJ, Decizia nr. 15/2013 privind judecarea recursului în interesul legii ce formează obiectul Dosarului nr. 12/2013, Publicat în Monitorul Oficial, Partea I nr. 760 din 06.12.2013.

677 Vezi explicații detaliate în capitolul "Tehnologia informațiilor și comunicațiilor", *supra*.

678 Pentru o prezentare detaliată a contaminanților informatici (*malware*), a se vedea I. Vasiu, L. Vasiu, *Criminalitatea în cyberspațiu*, op. cit., p. 93-99.

679 Pentru clasificare și detalii asupra acestora, a se vedea, I. Vasiu, L. Vasiu, *Criminalitatea în cyberspațiu*, op. cit., p. 99-107.

prevederea obiectivelor şi efectelor acestor contaminanţi informatici urmărite de făptuitori.

Cele mai actuale forme de *malware* sunt cele care fură date prin copiere şi le trimit către o altă adresă; cele care împiedică operaţiunile sistemelor de informaţii, inclusiv pe cele care controlează infrastructuri critice (cum ar fi sisteme vitale pentru societate: energie, apă, transport, etc); spre exemplu, un tip de *malware*, *ransomware* poate bloca accesul la date informatice sau împiedica folosirea sistemului informatic până când victima plăteşte suma cerută[680]. Folosirea pe scară din ce în ce mai largă a dispozitivelor mobile, a stimulat dezvoltarea de programe informatice de tip *malware* pentru acest tip de comunicaţii[681].

O formă foarte periculoasă, care implică programe informatice maliţioase, constă în crearea şi folosirea de *botnet*-uri. Conform Propunerii de Directivă a Parlamentului European şi a Consiliului privind atacurile împotriva sistemelor informatice şi de abrogare a Deciziei-cadru 2005/222/JAI a Consiliului, prin *botnet* se desemnează o reţea de calculatoare care au fost infectate cu programe ostile (contaminanţi informatici, numiţi *bot*[682]). Infectarea se poate face prin intermediul site-urilor de socializare[683], mesajelor de tip *spam*, mesajelor postate pe forumuri pe web sau prin descărcări de tip *drive-by*. O astfel de reţea de calculatoare infectate ("zombie") poate fi activată pentru a efectua acţiuni specifice, cum ar fi atacarea sistemelor informatice, calculatoarele infectate fiind controlate, adesea fără cunoştinţa utilizatorilor calculatoarelor afectate, de un alt calculator, cunoscut sub numele de „centrul de comandă şi control" (*command-and-control*).

Un tip de atac informatic frecvent întâlnit este reprezentat de *phishing*. Acest tip de atac este o formă de fraudă în care transmiţătorul impersonează organizaţii sau firme legitime în încercarea de a determina recipienţii să divulge informaţii personale, cum ar fi parole de acces sau numere de conturi, cu obiectivul final de a fura identitatea şi/sau banii celor păcăliţi[684]. În unele cazuri, numărul de victime şi/sau sumele obţinute în urma unor asemenea atacuri este foarte mare (spre exemplu, în *United States v. Blount*, au fost 250 de victime şi pierderi de peste 120.000 dolari)[685].

Cerinţele esenţiale. Pentru existenţa elementului material, la toate infracţiunile din acest capitol este necesar ca acţiunea, prin care se produce o lezare a atributelor securităţii sistemelor sau datelor informatice, să fie realizată "fără drept" sau "neautorizat". Această cerinţă este definită în conformitate cu

---

680 Acest tip de *malware* este disponibil şi pentru dispozitivele mobile - vezi, spre exemplu, cazul Android Defender, descris în Sophos, *Security Threat Report*, 2014, p. 8.

681 Vezi detalii în Sophos, op. cit.

682 Vezi Y. Namestnikov, *The economics of botnets*, 2009.

683 Vezi Europol, *Internet facilitated organised crime*, 2011.

684 Vezi K.R. Sahu şi J. Dubey, *A Survey on Phishing Attacks*, International Journal of Computer Applications, 88, 2014; Jian Mao şi colab., *BaitAlarm: Detecting Phishing Sites Using Similarity in Fundamental Visual Features*, 5th International Conference on Intelligent Networking and Collaborative Systems, IEEE, 2013; Symantec, *State of Spam & Phishing Report*, 2012.

685 United States v. Blount, No. 09-2139-cr (2d Cir. May 14, 2010).

BCU IASI / CENTRAL UNIVERSITY LIBRARY

recomandările din Convenţia europeană privind criminalitatea informatică, de art. 35, lit. h) din Legea nr. 161/2003. Astfel, în sensul prezentului capitol, acţionează „fără drept" persoana care se află în una dintre următoarele situaţii: a) nu este autorizată, în temeiul legii sau al unui contract; b) depăşeşte limitele autorizării; c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfăşura cercetări ştiinţifice sau de a efectua orice altă operaţiune într-un sistem informatic.

Urmarea imediată constă în constă în atingerea adusă oricăreia dintre atributele descrise în cadrul secţiunii dedicate obiectului juridic (confidenţialitatea, integritatea şi disponibilitatea datelor sau sistemelor informatice).

Legătura de cauzalitate. Între activitatea incriminată şi urmarea imediată trebuie să existe un raport de cauzalitate. De regulă, urmarea imediată rezultă din materialitatea faptelor (*ex re*). În unele cazuri, legea prevede şi condiţia producerii unei urmări concrete în urma atacului asupra sistemului informatic; spre exemplu, la infracţiunea prevăzută la art. 363 C. pen., este necesară producerea unei "perturbări grave a funcţionării sistemului informatic".

În cazul incriminărilor în care sunt prevăzute mai multe rezultate alternative, infracţiunea se consumă, în principiu, prin realizarea oricăreia din urmările imediate prevăzute de lege (spre exemplu, la infracţiunea de interceptare ilegală a unei transmisii de date informatice, prevăzută la art. 361 C. pen. în două variante alternative, cu rezultate alternative).

Fapta îşi păstrează caracterul unitar, reţinându-se săvârşirea unei singure infracţiuni dacă se produc mai multe rezultate alternative, în aceeaşi împrejurare. Când urmările alternative se produc în timp, ca urmare a unor acte separate, poate fi reţinut concursul de infracţiuni sau forma continuată, în funcţie de poziţia subiectivă a autorului faptelor.

Cu toate că, în principiu, raportul de cauzalitate ar trebui să fie uşor de identificat de organele judiciare, rezultând din materialitatea faptei, specificitatea mediului digital şi ingeniozitatea celor care comit infracţiuni informatice fac uneori dificilă stabilirea acestuia.

b) Latura subiectivă

Elementul subiectiv. Infracţiunile din acest capitol se comit cu intenţie directă sau indirectă.

Scopul. Cerinţa esenţială. În unele variante ale infracţiunilor din acest capitol, legiuitorul prevede şi o condiţie esenţială în legătură cu *scopul* realizării activităţii infracţionale ; spre exmplu, la infracţiunea de acces ilegal la un sistem informatic, prevăzută la art. 360 C. pen, la varianta agravată de la alin (2), legiuitorul prevede accesul ilegal săvârşit *în scopul obţinerii de date informatice* sau la infracţiunea de operaţiuni ilegale cu dispozitive sau programme informatice (art. 365 C. pen.), unde legiuitorul prevede ca activităţile făptuitorului să fie realizate *în scopul realizării infracţiunilor prevăzute în art. 360-364*.

Mobilul săvârşirii infracţiunilor nu constituie element component al laturii subiective, însă stabilirea acestora poate contribui, în fiecare caz concret, la o justă individualizare a pedepsei.

B.C.U. „M. EMINESCU" IAŞI

BCU IASI / CENTRAL UNIVERSITY LIBRARY

Forme, modalități, sancțiuni

A. Formele infracțiunii

a) **Actele pregătitoare.** Actele pregătitoare (procurarea sau realizarea de dispozitive vizând comiterea infracțiunilor din acest capitol) pot face obiectul unei infracțiuni autonome din acest capitol, dacă sunt îndeplinite condițiile cerute de lege: infracțiunea incriminată în art. 365 din noul Cod penal și anume accea de *operațiuni ilegale cu dispozitive sau programe informatice.*

b) **Tentativa** este posibilă și se pedepsește la toate infracțiunile din acest capitol conform art. 366 din noul Cod penal (acesta fiind conform art. 47 a Legii nr. 161/2003, sursa acestui articol din noul Cod penal).

c) **Consumarea** infracțiunilor are loc în momentul în care se realizează urmarea imediată prevăzută de lege.

d) **Epuizarea** are loc în momentul comiterii ultimului act al activității infracționale. Infracțiunile din acest capitol sunt susceptibile de a fi săvârșite în forma continuă sau continuată.

B. Modalități

Modalitățile normative sunt cele arătate în textul de incriminare și pot consta în multiple activități: *acces ilegal, intercepție ilegală, transfer neautorizat de date, alterare de date, restricționarea accesului la sistemul informatic sau la date, producere ilegală de programe sau dispozitive,* etc. Unele din infracțiunile prevăzute în acest capitol au, pe lângă *forma simplă* sau de bază, și *forme agravate.* Astfel de forme agravate întâlnim la infracțiunea de acces ilegal la un sistem informatic (art. 360, alin. 2 și alin. 3). O *atenuantă* este prevăzută la infracțiunea de operațiuni ilegale cu dispozitive sau programe informatice (art. 365, alin. 2).

Modalitățile de fapt. Toate aceste *modalități normative* se pot prezenta într-o varietate de *modalități de fapt.*

C. Sancțiuni

Legea prevede, pentru infracțiunile din acest capitol, pedepse cu închisoarea cuprinsă între limite moderate, uneori alternativ cu pedeapsa amenzii penale (cazul infracțiunilor prevăzute în art. 360 alin. 1 și art. 365, C. pen., alin.1 și 2). Infracțiunile prevăzute în acest capitol sunt sancționate diferit, în funcție de gravitatea faptei. Cea mai severă sancțiune este de închisoare de la 2 la 7 ani, acordată pentru o formă agravată la accesul ilegal la un sistem informatic și pentru infracțiunea de perturbarea funcționării sistemelor informatice. Infracțiunile care se săvârșesc prin modalități normative alternative, sunt sancționate între aceleași limite de pedeapsă, iar variantele normative sancționate cu pedepse similare sau diferite. De asemenea, sunt reglementate și forme agravate la unele infracțiuni, și o formă atenuată, limitele de pedeapsă prevăzute pentru infracțiunea tip fiind majorate, respectiv reduse corespunzător.

Semnalăm o îmblânzire nejustificată a aproape tuturor sancțiunilor pentru infracțiunile din acest capitol în comparație cu cele corespunzătoare din Legea nr. 161/2003. La nivel european și global se consideră că

BCU IASI CENTRAL UNIVERSITY LIBRARY

periculozitatea și consecințele acestor infracțiuni cer sancțiuni aspre din partea legiuitorilor naționali (mai ales într-o țară ca România, considerată în multe rapoarte și statistici "un rai al hackerilor")[686].

Explicații complementare

A. Legătura cu alte infracțiuni. Asemănările sau deosebirile dintre aceste infracțiuni sunt relevate cu ușurință prin compararea textelor în discuție. Având în vedere că valoarea centrală apărată prin prevederile din acest capitol este *securitatea informatică*, cu cele trei atribute fundamentale (*integritatea, confidențialitatea, disponibilitatea*), este ceea ce le distinge de alte infracțiuni care protejează alte atribute afectate prin atacurile informatice (spre exemplu, securitatea națională, securitatea internațională, viața privată, secretul corespondenței, securitatea tranzacțiilor electronice, securitatea și inviolabilitatea sistemelor electronice de tranzacționare, de depozitare sau de compensare-decontare în cadrul pieței de capital, ocrotirea drepturilor de proprietate intelectuală, în special a drepturilor de autor etc.).

Unele infracțiuni contra siguranței și integrității sistemelor informatice sunt *subsidiare* față de altele datorită caracterului lor de generalitate (spre exemplu, accesul ilegal la un sistem informatic), astfel că dacă o faptă comisă în realitate realizează și conținutul unei incriminări cu caracter special – cu o sferă de cuprindere mai redusă datorită condițiilor în plus incluse în conținutul constitutiv, se va reține această din urmă infracțiune, aplicându-se regula potrivit căreia generalul este subsidiar specialului.

Un astfel de exemplu ar fi infracțiunea incriminată de art. 32, lit. q) din Legea nr. 535/2004 privind prevenirea și combaterea terorismului, articol modificat și completat de art. 159 din Legea 187/2012 pentru punerea în aplicare a Legii nr. 286/2009, *fraude comise prin sisteme informatice și mijloace de plată electronice și infracțiuni contra siguranței și integrității sistemelor și datelor informatice*; astfel, dacă oricare din infracțiunile cuprinse în cele două categorii cuprinse mai sus sunt comise în condițiile prevăzute de legea privind prevenirea și combaterea terorismului, vor fi incidente aceste prevederi, și nu cele din capitolul de față privitor la siguranța și integritatea sistemelor și datelor informatice.

Un alt exemplu, în acest sens, este și infracțiunea incriminată de Legea nr. 297/2004[687] privind piața de capital - *accesul ilegal la un sistem electronic de tranzacționare* (o variantă de specie a accesului ilegal la un sistem informatic, prevăzut de noul Cod penal în grupa de infracțiuni contra siguranței și integrității sistemelor informatice). În acest caz, se va reține infracțiunea incriminată de Legea

---

[686] Vezi, spre exemplu, *Romanian Town Nicknamed Hackerville*, 2013, disponibil la http://www.govtech.com/security/Romanian-Town-Nicknamed-Hackerville.html, unde se afirmă că infractori din România au furat de la entități din SUA circa 1 miliard de dolari numai în 2012.

[687] Art. 279, alin.1, lit c). Se pedepsește cu închisoare de la 6 luni la 5 ani și interzicerea unor drepturi accesarea cu intenție de către persoane neautorizate a sistemelor electronice de tranzacționare, de depozitare sau de compensare-decontare (articol modificat prin art. 152, pct. 3 din Legea nr. 187/2012 pentru punerea în aplicare a Legii nr. 286/2009).

nr. 297/2004[688] privind piaţa de capital - *accesul ilegal la un sistem electronic de tranzacţionare*, aplicându-se regula potrivit căreia generalul este subsidiar specialului. Într-un caz din aprilie 2014, o grupare infracţională specializată în manipularea pieţei de capital şi înşelăciuni cu consecinţe deosebit de grave, a fost investigată pentru savârşirea infracţiunilor de iniţiere, constituire, aderare şi sprijinire a unui grup infracţional organizat, manipulare a pieţei de capital, înşelăciune cu consecinţe deosebit de grave, fals informatic şi *acces ilegal la un sistem electronic de tranzacţionare*, prejudiciul cauzat prin activităţile ilicite fiind estimat la 3.000.000 lei[689].

În numeroase cazuri, aceste infracţiuni intră în concurs ideal sau real cu alte infracţiuni. Astfel, spre exemplu, în vederea pregătirii săvârşirii fraudelor prin mijloace de plată electronice (infracţiuni privind comerţul electronic preluate din Legea nr. 365/2002 privind comerţul electronic în noul Cod penal la Titlul II, Infracţiuni contra patrimoniului, Cap. IV, Fraude comise prin sisteme informatice şi mijloace de plată electronice), se pot săvârşi infracţiuni îndreptate împotriva securităţii datelor sau sistemelor informatice, cum este şi aceea de acces ilegal într-un sistem informatic.

Aşadar, accesul ilegal în sistemul informatic se face, de regulă, în scopul săvârşirii uneia sau mai multora dintre aceste infracţiuni de fraudă menţionate mnai sus (cel mai frecvent este vorba de infracţiunea de Efectuarea de operaţiuni financiare în mod fraudulos, prevăzută de noul Cod penal la art. 250), situaţie care justifică reţinerea unui concurs cu conexitate etiologică în care accesul ilegal reprezintă mijlocul prin care se realizează scopul şi anume efectuarea de operaţiuni financiare în mod fraudulos.

B. Aspecte procesuale. Pentru toate infracţiunile prevăzute în acest capitol, acţiunea penală se pune în mişcare din oficiu. iar urmărirea penală este efectuată de către organele de cercetare penală, sub supravegherea procurorului.

C. Precedente legislative şi situaţii tranzitorii

a) **Precedente legislative.** Infracţiunile componente ale acestui capitol sunt în totalitate preluate (cu o mică modificăre de sistematizare, respectiv o detaliere a unui termen-cheie) din Legea nr 161/2003, a cărei sursă este Convenţia europeană privind criminalitatea informatică.

b) **Situaţii tranzitorii.** Limitele de pedeapsă fiind mai reduse în noul Cod penal (cu o excepţie minoră: în cazul art. 360, varianta de bază şi prima formă agravată, limitele de pedeapsă sunt la fel), în cazul succesiunii de legi penale în timp se va face aplicarea dispoziţiilor din noul Cod penal.

---

688 Art. 279, alin.1, lit c.) Se pedepseşte cu închisoare de la 6 luni la 5 ani şi interzicerea unor drepturi accesarea cu intenţie de către persoane neautorizate a sistemelor electronice de tranzacţionare, de depozitare sau de compensare-decontare (articol modificat prin art. 152, pct. 3 din Legea nr. 187/2012 pentru punerea în aplicare a Legii nr. 286/2009).

689 A se vedea, detalii la locaţia http://observator.ro/248443/perchezitii-la-constanta-intr-un-caz-de-inselaciune-la-bursa-248443.html.

Elemente de drept comparat

În propunerea de Tratat global în domeniul cybersecurității și cybercriminalității[690], infracțiunile care fac parte din acest capitol al noului Cod penal sunt prezente toate sub titlul de *Infracțiuni contra integrității, confidențialității și disponibilității sistemelor și datelor informatice*, sursa de inspirație fiind Convenția europeană în domeniul criminalității informatice. Intenția ONU este de a avea la nivel global aceleași reglementări, acest lucru facând posibilă tragerea la răspundere a tuturor celor care comit aceste infracțiuni, cunoscut fiind caracterul preponderent transfrontalier al acestui tip de criminalitate.

Având în vedere faptul că aceste infracțiuni sunt prevăzute în zeci de legislații în aceeași formă, de multe ori perfect identică (82 de țări din lume au semnat și ratificat un instrument legal regional în domeniu, iar dintre acestea peste 40 au utilizat ca model Convenția europeană în domeniul criminalității informatice[691]) având aceeași sursă, prezentăm numai câteva prevederi naționale relevante în domeniu, cu titlu de exemplu. De fapt, o problemă mare a fost până acum implementarea acestor prevederi în practică, tehnicitatea termenilor utilizați cerând o expertiză corespunzătoare a organelor judiciare.

Se consideră la nivel global că nu este nevoie de detalieri suplimentare ale textelor de lege, aceste reglemnentări fiind pe de o parte neutre din punct de vedere tehnologic, iar de de altă parte, noile generații născute în era digitală înțeleg mediul, formele și particularitățile acestui tip de criminalitate fără probleme, având în vedere faptul că utilizează sistemele informatice pentru toate activitățile zilnice: recreere, educație, lucru, servicii, etc.

Legislația franceză în materie. Franța a semnat Convenția europeană privind criminalitatea informatică în 23 noiembrie 2001 și a ratificat-o în 5 martie 2007 prin Legea nr. 297/2007.

Prima lege franceză în domeniu, No. 88-19, numită și *Godfrain*, privea frauda informatică și a fost adoptată în anul 1988. În timp, Parlamentul francez a adoptat mai multe legi cu relevanță în acest domeniu. În prezent, majoritatea prevederilor referitoare la criminalitatea informatică sunt cuprinse in Codul penal francez, Cartea a III-a, Titlul II, Capitolul III al Părții speciale, referitor la atacurile asupra sistemelor informatice. Cu toate că Franța a ratificat Convenția europeană în domeniul criminalității informatice, nu toate prevederile ei au au fost preluate în structura- model din reglementarea europeană: de exemplu, pentru frauda informatică și falsul informatic, sunt aplicabile textele tradiționale referitoare la excrocherie (art. 313-1 Cod penal francez), respectiv fals (art. 441-1 Cod penal francez).

Cadrul legal francez este unul dintre cele mai complete și complexe în domeniu: cuprinde *hacking*-ul (art. 323-1), *cracking*-ul (323-1), introducerea de coduri malițioase care cauzează modificarea de date (art. 323-3 Cod penal).

---

690 Vezi detalii în I. Vasiu și L. Vasiu, *Criminalitatea în cyberspațiu*, 2011, p. 121- 138.

691 A se vedea, United Nations Office for Drugs and Crimes, *Comprehensive Study on Cybercrime*, draft, 2013, pag. XIX.

Instalarea de programe ilegale, cum ar fi *spyware* sau *sniffer*[692], este prevăzută în art. 323-1, *phishing-ul* este prevăzut în art. 226-18, 321-3, iar în art. 434-23 reglementează uzurparea identităţii (sau *furtul de identitate*) şi unele prevederi privitoare la proprietatea intelectuală (contrafacerea marcilor). De asemenea, legislaţia penală franceză prevede şi sancţionează şi *spam*-ul (trimiterea de mesaje electronice nesolicitate) în Legea nr. 575/2004; spam-ul este prevăzut şi sancţionat şi de codul penal (art. 323-2).

Codul penal francez prevede în art. 323-1 accesul ilegal la un sistem informatic, precizând că poate să fie acces în tot sau în parte; de asemenea, la accesul ilegal este prevăzută cerinţa ca intrarea să fie frauduloasă, iar o modalitate a acestui comportament criminal se poate manifesta prin încălcarea măsurilor de securitate. În art. 323-2 Cod penal este prevăzută perturbarea funcţionării sistemelor informatice (sau sabotajul informatic).

Legislaţia italiană în materie. Codul penal italian a fost completat cu prevederi în domeniul infracţiunilor informatice de tipul celor prevăzute în noul nostru Cod penal la capitolul de faţă, înainte de implementarea Convenţia europeană în domeniul criminalităţii informatice, cu reglementările din Legea italiană privitoare la criminalitatea informatică din 1993 (Act No. 547, 1993) şi după aceea, prin Legea nr.48/2008, devenind una dintre cele mai complexe şi complete reglementări actuale în acest domeniu. Spre exemplu: accesul ilegal (abuziv) la un sistem informatic este prevăzut în art. 615ter şi are ca sursă art. 4 din Legea nr. 547 din 23.1.1993; posesia ilicită a unui cod de acces la un sistem informatic sau de telefonie este prevăzută în Art. 615-*quater*.

În deplin acord cu prevederile Convenţiei europene în domeniu, Codul penal italian conţine pe lângă cele de mai sus, prevederi referitoare la toate infracţiunile din acest capitol: în art 635–*quarter* şi 635-*quinquies* prevede perturbarea funcţionării sistemelor informatice, în art. 635-*bis* şi art. 635-*ter* - alterarea integrităţii datelor informatice, în art. 617-*quarter*, art 617- *quinquies*, art. 617-*sexies* şi art. 623-*bis*, interceptarea ilegală.

Reglementarea italiană din 1993 a adăugat mai multe articole în domeniul criminalităţii informatice în Codul Penal italian caracterizate prin complexitate, dar unele părţi au fost considerate prea generale şi vagi, făcând dificilă interpretarea şi aplicarea în practică (aşa cum s-a întâmplat şi cu legislaţia românească în domeniu). Acest act legislativ conţine douăsprezece puncte privitoare la o serie de activităţi criminale realizate prin sau asupra calculatoarelor, incluzând accesul ilegal la sistemele infornatice, distrugerea sau deterioararea intenţionată a sistemelor informatice, operaţiunile ilegale cu parole sau coduri de acces, crearea sau distribuirea de viruşi, viermi şi crearea de înscrisuri electronice false; de asemenea, există prevederi pentru protecţia bazelor de date, copierea ilegală a topografiilor de cip, utilizarea neautorizată a codurilor cărţilor de credit sau cartelelor telefonice, parolelor sau conturilor bancare.

---

[692] *Spyware* este o categorie de programe maliţioase, infiltrate pe un anumit sistem informatic, care monitorizează în mod secret utilizatorii sistemului infectat, permiţând obţinerea de informaţii senzitive, cum ar fi parole sau date financiare. *Sniffer* (numit şi *packet sniffer*) este o altă categorie de program maliţios, care permite interceptarea fluxului de date într-o reţea.

BCU IASI CENTRAL UNIVERSITY LIBRARY

Legea italiană din 1993 este împărțită în mai multe părți, fiecare privind diferite activități criminale in domeniul informatic. Prima parte, în particular, primele patru articole, se referă la posesia, alterarea sau distrugerea de date sau sisteme informatice. A doua parte privește accesul neautorizat sau piratat la sistemele informatice și interceptarea ilegală a comunicațiilor electronice.

A treia parte a Legii nr. 547/1993 privește falsificarea unei comunicați electronice, distribuirea de viruși, posesia ilegală a dispozitivelor de interceptare sau perturbare a comunicațiilor, precum și divulgarea de informații confidențiale. Toate aceste infracțiuni erau sancționate cu închisoare până la 6 ani. Prima dată când aceste prevederi au fost puse în vigoare în anul 1994, când statul italian a început o operațiune masivă, denumită "Hardware", prima operațiune italiană la nivel național împotriva crimelor informatice și violărilor în domeniul dreptului de autor.

Această lege, din 1993, a fost completată și modificată în timp, ținându-se cont de tendințele criminalității informatice (în 1998, Legea italiană privind pornografia infantilă; Legea Internetului nr. 269 din 3 august 1998; Legea aprobată de Consiliul de Miniștri în 7 noiembrie 2003; codul de autoreglementare. Internet și minori, etc.).

Codul penal austriac prevede în Secțiunea 126 C infracțiunea de operațiuni ilegale cu operațiuni sau programe informatice, în Secțiunea 126 B perturbarea funcționării sistemelor informatice (sau sabotajul informatic), în Secțiunea 126 a, alterarea integrității datelor informatice, iar în Art. 119- 119 a, accesul ilegal la un sistem informatic.

Legislația SUA. SUA este una dintre țările din afara Europei care a semnat și ratificat Convenția europeană în domeniul criminalității informatice. La nivel federal, infracțiunile contra confidențialității integrității și disponibilității sistemelor și datelor informatice sunt prevăzute în 18 U.S.C. § 1030 (*Computer Fraud and Abuse Act*), din anul 1986, modificat de mai multe ori subsecvent[693], în următoarea sistematizare: (1) obținerea neautorizată de informații privind securitatea națională; (2) obținerea neautorizată de informații de la o instituție financiară, departament sau agenăie a Statelor Unite sau de pe orice calculator protejat; (3) accesul neautorizat la calculatoare guvernamentale; (4) frauda informatică; (5) perturbarea sistemelor informatice (*computer damage*); (6) traficarea de parole; (7) șantajul prin mijloace informatice.

De menționat că, deși există critici legate de modul vag de prevedere a unor termeni-cheie (care face dificilă implementarea de către instanțe în cazuri concrete), precum și de unele prevederi de drept procedural, SUA consideră Convenția cel mai potrivit instrument legal la nivel internațional în domeniu[694].

---

693 Vezi Pamela Taylor, *To Steal or Not to Steal: An Analysis of the Computer Fraud and Abuse Act and Its Effect on Employers*, 49 Hous. L. Rev. 201, 207, 2012; David J. Rosen, *Limiting Employee Liability Under the CFAA: A Code-Based Approach to "Exceeds Authorized Access*, 27 Berkeley Technology Law Journal 737, 738, 2012.

694 A se vedea, Amalie M. Weber, *The Council of Europe's Convention on Cybercrime*, Berkeley Technology Law Journal, vol.18, 425, 2003.

4.6.2 Accesul ilegal la un sistem informatic

Art. 360. (1) - Accesul, fără drept, la un sistem informatic se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă.
(2) - Fapta prevăzută în alin. (1), săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoarea de la 6 luni la 5 ani.
(3) - Dacă fapta prevăzută în alin. (1) a fost săvârşită cu privire la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, accesul este restricţionat sau interzis pentru anumite categorii de utilizatori, pedeapsa este închisoarea de la 2 la 7 ani.

Aspecte generale

Această infracţiune nu exista în vechiul Cod penal, infracţiunea fiind reprodusă, fără modificări semnificative, din Legea nr. 161/2003. În art. 42 al Legii nr. 161/2003, în debutul Secţiunii *1 – Infracţiuni contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice*[695], legiuitorul a prevăzut infracţiunea de *acces ilegal la un sistem informatic*. Infracţiunea din art. 42 era prevăzută într-o formă simplă (de bază), care interzice accesul fără drept la un sistem informatic (alin. 1) şi două variante agravante, care constau în săvârşirea faptei de la alin. 1 în scopul obţinerii de date informatice (alin. 2), respectiv prin încălcarea măsurilor de securitate (alin. 3).

În noul Cod penal, legiuitorul reformulează varianta de la alin. (3), aceasta constând în fapta prevăzută în alin. (1), dacă a fost săvârşită cu privire la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, accesul este restricţionat. Modificarea nu este semnificativă, având în vedere faptul că legiuitorul descrie de fapt prin utilizarea conceptelor: "proceduri", "dispozitive" sau "programe", măsurile de securitate fizică sau de securitatea informaţiei la care se referă conceptul "măsuri de securitate" folosit în Legea nr. 161/2003.

Remarcăm, chiar din titlul capitolului din care face parte această infracţiune, preferinţa legiuitorului pentru folosirea altui termen decât *securitatea informatică* (de menţionat că acesta din urmă este cel consacrat la nivel global şi în legislaţia referitoare la securitatea informatică şi în cea referitoare la criminalitatea informatică[696]), şi anume cel de "siguranţă". Preferinţa legiuitorului vine, credem noi, mai mult din faptul de a potrivi titlul acestei grupe cu cel al categoriei din care face parte, şi anume: *Infracţiuni contra siguranţei publice*. Considerăm alegerea legiuitorului pentru denumirea acestui capitol discutabilă, având în vedere că dă impresia greşită că acoperă numai un aspect al securităţii informatice (integritatea)

[695] De remarcat că legiuitorul a preluat numai parţial titlul subgrupei din Convenţia europeană, omiţând un concept/element cheie: disponibilitatea datelor şi sistemelor informatice – vezi Convenţia privind criminalitatea informatică, Titlul 1: *Offences against the confidentiality, integrity and availability of computer data and systems*.

[696] A se vedea, spre exemplu, Cybercrime Convention (2001) Titlul I Offences against integrity, confidentiality and disponibility, *New Global Treaty on cybersecurity and cybercriminality*, ENISA (Agenţia europeană cu privire la securitatea reţelelor).

BCU IASI / CENTRAL UNIVERSITY LIBRARY

şi este, pe de cealaltă parte şi redundantă (integritatea este o parte a securităţii informatice or a siguranţei). Chiar Directiva din 2013 de la nivelul Uniunii Europene în materia atacurilor asupra sistemelor informatice utilizează termenul de securitate informatică[697], cu cele trei aspecte esenţiale definitorii: integritate, confidenţialitate şi disponibilitate.

Concept şi caracterizare

În cadrul mijloacelor de protecţie împotriva atacurilor în mediul electronic se înscriu şi prevederile penale consacrate de noul Cod penal. Răspunzând obligaţiilor asumate faţă de comunitatea internaţională, România şi-a adaptat legislaţia penală pentru a reflecta schimbările datorate progresului tehnologic, ţinând seama de prevederile Convenţiei europene privind criminalitatea informatică[698]. Asigurarea unui nivel adecvat de protecţie a sistemelor informatice ar trebui să facă parte dintr-un cadru cuprinzător şi eficace de măsuri de prevenţie care să completeze măsurile prevăzute de drept penal ca răspuns la criminalitatea informatică.

Legea penală română incriminează în art. 360 din noul Cod penal accesul ilegal la un sistem informatic într-o formă simplă şi două forme agravante care sunt preluate fără modificări semnificative din Legea nr. 161/2003 (se modifică doar pedeapsa la varianta agravată prevăzută la alin. 3 şi configuraţia unei variante agravate), care, la rândul ei, reproduce textul din art. 2 al Convenţiei europene privind accesul ilegal la un sistem informatic.

Infracţiunea de acces ilegal la un sistem informatic nu deschide în mod întâmplător această grupă de infracţiuni informatice, ea fiind considerată cea mai importantă, o adevărată "infracţiune de bază", care permite comiterea altor infracţiuni cu care intră în concurs (spre exemplu, falsul informatic, frauda informatică etc.). Precizăm, în acest context, importanţa definirii precise şi detaliate a termenilor cheie utilizati de legiuitor (spre exemplu: "sistem informatic", "acces", "date informatice", "măsuri de securitate", "fără drept"). Interpretarea defectuoasă a acestor termeni, a dus la un deceniu de practică neunitară, cu soluţii diferite sau chiar defectuoase, în cazuri similare, ceea ce a necesitat promovarea unui Recurs în Interesul Legii in 2013[699].

Accesul ilegal la un sistem informatic mai este întâlnit şi sub denumirea de *hacking*[700] şi poate include trecerea de o parolă sau de un alt mecanism de protecţie a unui sistem sau a unor date informatice, pentru a obţine acces la acestea fără autorizare. Această infracţiune a devenit un fenomen de masă, cu victime celebre,

---

697 Vezi Directiva 2013/40/UE a Parlamentului European şi a Consiliului din 12 august 2013.

698 Lucrările la elaborarea acestei Convenţii au debutat în noiembrie 1996, când Comitetul European pe probleme criminale, prin Decizia CDPC/103/211196, a hotărât înfiinţarea unui Comitet de experti care să se ocupe de problema criminalităţii informatice. În anul 2001, Convenţia europeană în domeniul criminalităţii a fost deschisă statelor pentru semnare, România fiind una dintre ţările semnatare ale aceastei Convenţii.

699 A se vedea Înalta Curte de Casaţie şi Justiţie (ÎCCJ), Decizia nr. 15/2013 privind judecarea recursului în interesul legii ce formează obiectul Dosarului nr. 12/2013 (Monitorul Oficial, Partea I nr. 760 din 06.12.2013).

700 Vezi ITU, *Electronic Crimes: Knowledge–based Report* (Assessment), 2013, p. 29.

cum ar fi: United States Airforce, Pentagon, Guvernul german, companiile Yahoo, Google, e-Bay, etc.[701]

Intruziunile de acest tip permit infractorilor să obţină access la parole, date bancare, personale sau clasificate (strict confidenţiale). Spre exemplu, în *Operation Ghost Stories*, 10 ruşi au spionat în SUA; în cazul Gowadia, au fost transmise în China informaţii privind apărarea naţională a SUA şi date militare tehnice. În *United States v. Valle*[702], deşi făptuitorul, în calitate de ofiţer de poliţie, a fost autorizat sa acceseze date pe un anumit sistem informatic, nu a fost autorizat să acceseze date despre o anumită persoană, el neavând motiv legal valid pentru a obţine asemenea date, depăşirea autorizării acordate fiind incriminată de 18 U.S.C. § 1030(a)(2)(B).

În România, un individ din Arad, cunoscut sub numele de "Guccifer", a accesat ilegal conturi de Facebook şi e-mail ale mai multor persoane publice, fiind reţinut pentru comiterea a 25 de infracţiuni de acces fără drept la sisteme informatice[703]. Într-un caz, un individ a fost condamnat la un an şi jumătate de închisoare pentru săvârşirea infracţiunii de acces ilegal la un sistem informatic, după ce a modificat fără drept parola de acces şi setările de securitate ale contului de poştă electronică aparţinând unei societăţi la care fusese angajat[704]. Într-un alt caz, Cristian Cioacă a fost condamnat la trei ani de închisoare cu suspendare, pentru acces ilegal la sisteme informatice, restricţionare ilegală a accesului la date informatice şi transferul neautorizat de date informatice, în timp ce hackerul care l-a ajutat să spargă e-mail-ul în cauză a primit o pedeapsă de un an şi jumătate cu suspendare[705].

"Access" înseamnă intrare în orice parte a unui sistem informatic, cum ar fi componentele hardware sau datele stocate, dar nu include, aşa cum se menţionează în Raportul explicativ al Convenţiei europene "simpla trimitere a unui mesaj de e-mail către un sistem (*file system*)". Accesul include şi intrarea într-un alt sistem informatic conectat via o retea publică de telecomunicaţii sau conectat la aceeaşi reţea (LAN - reţea locală de comunicaţii) sau un intranet al aceleiaşi organizaţii. Accesul poate fi considerat ilegal şi în situaţii în care se depăşeşte autorizarea acordată sau se realizează după revocarea autorizării de acces a sistemului informatic[706].

Încriminarea din noul Cod penal corespunde de principiu cerinţei inserate în Directiva 2013/40/UE a Parlamentului European şi a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice şi de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului şi anume ca "statele membre adoptă măsurile

---

[701] Unele din atacurile asupra acestor victime bine-cunoscute au fost comise de hackeri români; spre exemplu, Călin Mateiaş, Butika Robert, hackerul din Arad, poreclit Guccifer, etc.

[702] United States v. Valle, No. 12 cr 847 (PGG) (S.D.N.Y. June 30, 2014).

[703] A se vedea detalii la locaţia: http://adevarul.ro/locale/arad/hackerul-guccifer-zis-micul-fum-fost-trimis-judecata-procurorii-diicot-1_532959940d133766a808b8ca/index.html.

[704] A se vedea detalii în Claudia Petraru, *Pentru acces ilegal la un sistem informatic, Condamnat la un an şi jumătate de închisoare*, disponibil la: http://www.obiectivtulcea.ro/pentru-acces-ilegal-la-un-sistem-informatic-condamnat-la-un-an-si-jumatate-de-inchisoare.html.

[705] A se vedea detalii la locaţia: http://www.flagrantct.ro/cristian-cioaca-a-fost-condamnat-la-trei-ani-de-inchisoare-cu-suspendare/.

[706] Vezi cazuri şi o discuţie detaliată în Ioana Vasiu şi Lucian Vasiu, *Break on Through*, op. cit.

necesare pentru a garanta că accesarea cu intenţie şi fără drept a unui sistem informatic sau a unei părţi a acestuia este incriminată atunci când este săvârşită prin încălcarea unei măsuri de securitate, cel puţin atunci când nu reprezintă un caz minor".

Elemente preexistente

A. Obiectul juridic al infracţiunii îl constituie relaţiile sociale a căror naştere şi dezvoltare este condiţionată de siguranţa şi integritatea sistemelor informatice sau, cum mai exact precizează legiuitorul european în Convenţia privind criminalitatea informatică, confidenţialitatea, integritatea şi disponibilitatea sistemelor informatice. Aceste trei elemente fundamentale ale securităţii sistemelor şi datelor informatice apar şi în propunerea de Tratat global privind securitatea şi criminalitatea informatică.[707]

Sistemele informatice joacă un rol vital în organizaţiile moderne pentru că ele furnizează informaţia necesară şi capacităţile de prelucrare şi diseminare a acesteia, strict necesare pentru îndeplinirea cerinţelor funcţionale/operaţionale, indiferent de context sau domeniul de activitate. Deoarece infracţionalitatea informatică poate avea consecinţe multiple, în unele cazuri foarte grave (putând afecta chiar economia sau securitatea naţională), precum şi pentru a asigura încrederea absolut necesară desfăşurării activităţilor care implică sisteme informatice şi pentru a respecta cerinţele legale existente, managementul securităţii sistemelor informatice devine extrem de important.[708]

Securitatea în domeniul sistemelor informatice se referă, în primul rând, la *confidenţialitate*, *integritate* şi *disponibilitate*. Pentru a evita repetarea, cu privire la prezentarea detaliată a celor trei componente fundamentale a securităţii sistemelor şi datelor informatice, facem trimitere la cele expuse în capitolul "Tehnologia informaţiilor şi comunicaţiilor".

B. Obiectul material constă în entităţile materiale care reprezintă sistemele informatice sau cele pe care sunt stocate informaţiile. În cazul variantei de la alin. 2, obiectul material constă în principal în entitatea materială pe care sunt stocate datele informatice şi asupra căreia se indreaptă activitatea incriminată. Entitatea materială pe care sunt stocate datele poate să îmbrace diverse forme: stick-uri de memorie (*USB flash*), discuri dure, discuri compact, discuri optice, memorii cu acces aleator etc.[709]

În cazul variantei de la alin. 3, obiectul material este reprezentat de dispozitivele sau entităţile materiale care stochează programe informatice sau mecanismele de securitate, menite să protejeze datele informatice şi sistemele informatice.

---

707 Vezi pentru detalii, I. Vasiu, L.Vasiu, *Criminalitatea în cyberspaţiu*, op. cit.

708 *Id.*

709 Pentru definiţii şi detalii privind aceste entităţi materiale, a se vedea I. Vasiu şi L. Vasiu, *Informatică juridică şi Drept informatic 2009*, op. cit.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

A. **Subiecţii infracţiunii**

a) **Subiect activ** poate fi orice persoană (fizică sau juridică) care are capacitate penală, textul de lege neprevăzând nici o calitate specială pentru aceasta. De regulă, însă, autorul este o persoană care are aptitudini sau cunoştinţe tehnice în domeniul calculatoarelor, o anumită familiaritate cu sistemele de securitate informatică şi vulnerabilităţile acestor sisteme sau persoane care sunt angajaţi ai entităţilor detinatoare ale sistemelor informatice (utilizatori de orice tip, care depăşesc nivelul de acces permis).

Participaţia penală este posibilă sub toate formele: coautorat, complicitate sau instigare.

b) **Subiect pasiv** al infracţiunii este persoana fizică sau juridică ce are în proprietate sistemele informatice şi al cărui drept la integritatea, confidenţialitatea şi/sau disponibilitatea sistemelor sau datelor informatice a fost încălcat sau periclitat.

Structura şi conţinutul juridic al infracţiunii

Aceasta este alcătuită dintr-o **situaţie premisă** şi un **conţinut constitutiv** al infracţiunii.

A. **Situaţia premisă**

Pentru ca infracţiunea de acces ilegal la un sistem informatic să poată fi săvârşită trebuie să existe o situaţie prealabilă (situaţia premisă), care presupune: existenţa unui sistem informatic (precum şi a reţelelor de calculatoare la care sunt conectate majoritatea covârşitoare a calculatoarelor) şi/sau a unor date informatice, asupra cărora făptuitorul să acţioneze fără drept, neautorizat sau depăşind autorizarea, în modalităţile prevăzute pentru realizarea scopului prevăzut în textul de lege.

Pentru a evita repetarea, cu privire la prezentarea detaliată a noţiunilor de "sistem informatic", "date informatice", "reţea", facem trimitere la cele expuse în capitolul "Tehnologia informaţiilor şi comunicaţiilor".

Pentru forma agravată de la alin. 3, situaţia premisă constă în **măsurile de securitate** (proceduri, dispozitive sau programe specializate) implementate de titularul sistemului informatic şi/sau a datelor, sau o persoană desemnată sau legitimată de acesta pentru a restricţiona sau interzice accesul pentru anumite categorii de persoane.

În art. 35, lit. h) din Legea nr 161/2003 sunt definite măsurile de securitate; prin acestea se înţelege folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restricţionat sau interzis pentru anumite categorii de utilizatori. Măsurile de securitate pot fi implementate pe două niveluri: securitatea sistemelor de calcul şi securitatea informaţiilor. Măsurile de securitate informatică pot fi clasificate ca *tehnice* şi *administrative*.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

A. Conținutul constitutiv al infracțiunii

a) Latura obiectivă a infracțiunii de acces ilegal la un sistem informatic cuprinde: elementul material, urmarea imediată, o cerință esențială, și legătura de cauzalitate între activitatea ilicită și rezultatul produs.

Elementul material al variantei normative de bază a infracțiunii constă în acțiunea de *acces* la un sistem informatic. Accesul ilegal[710] la un sistem informatic reprezintă o "platformă", o "poziționare" a atacatorului și este considerat, în majoritatea jurisdicțiilor, infracțiunea ce face posibilă realizarea majorității celorlalte infracțiuni informatice[711]. Spre exemplu, hacker-ul Guccifer, a realizat acces fără drept la un sistem informatic, după care a restricționat accesului la date informatice și a transferat neautorizat date sistem informatic[712].

Noțiunea de "acces" a ridicat și continuă să ridice numeroase probleme, atât la nivel de comentatori legali[713], cât și în instanțe[714]. Prin "acces" se înțelege intrarea în tot sau într-o parte a unui sistem informatic, capacitatea de a lansa comenzi, de a accesa date informatice sau de a efectua alte operațiuni informatice, fie direct de la o tastatură, fie prin intermediul unui rețele informatice.

Într-o formulare sintetică, definiția noastră a "accesului la un sistem informatic" este *capacitatea de a citi, scrie sau executa fișiere*, cu precizarea că a "scrie", în contextul sistemelor informatice, include capacitatea de a șterge un fișier[715]. După cum se precizează în Convenția europeană privind criminalitatea informatică, simpla trimitere a unui mesaj electronic sau fișier către un sistem informatic nu poate fi considerată "acces". Metoda folosită pentru realizarea accesului ilegal nu prezintă relevanță pentru existența infracțiunii[716].

Cerința esențială. Legiuitorul penal prevede în legătură cu activitatea incriminată condiția esențială ca aceasta să se desfășoare *fără drept*. În sensul

---

710 Prin "access" la un sistem informatic se înțelege capacitatea de a da comenzi, de a cauza introducerea, obținerea, afișarea, stocarea ori diseminarea de date informatice sau folosirea în orice alt mod a resurselor unui calculator, sistem sau rețea informatică, sau comunicarea cu unitățile sale aritmetice, logice sau de memorie.

711 Vezi S. Schjolberg, *The legal framework - Unauthorized access to computer systems*, 2003.

712 A se vedea detalii la locația: http://citynews.ro/eveniment/hackerul-vedetelor-trimis-judecata-1262244.

713 A se vedea K. M. Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, Note, 107 Michigan Law Review 819, 2009, p. 849–52; O. S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. Law Review, 2003; O. S. Kerr, *Computer Crime Law*, Thomson West, 2006.

714 Vezi, spre exemplu, *Court Rules Unauthorized Access to Computers Cannot Be "Double-Counted" to Constitute Felony*, The Computer & Internet Lawyer, Vol. 28, No. 7, July, 2011; M. Eichten, *The Computer Fraud and Abuse Act-A Survey of Recent Cases*, The Business Lawyer, 66. 1, 2010, p. 231-236.

715 A se vedea Ioana Vasiu, Lucian Vasiu, *The Cybercrime Challenge: Does the Romanian Legislation Answer Adequately?*, Law Review: Judicial Doctrine & Case-Law, 3.2, 2013.

716 A se vedea Ioana Vasiu, Lucian Vasiu, *Criminalitatea în cyberspațiu*, op. cit.; Lucian Vasiu, Ioana Vasiu, *Contaminanții informatici ca vector al accesului ilegal*, Revista de Drept Penal, 2006, p. 37-40; Lucian Vasiu, Ioana Vasiu, *Dissecting Computer Fraud: From Definitional Issues to a Taxonomy*, Proceedings of the 37th Hawaii International Conference on System Sciences, Big Island, Hawaii, USA, IEEE Computer, 2004.

prezentului articol, acţionează fără drept persoana care se află în una dintre următoarele situaţii: a) nu este autorizată, în temeiul legii sau al unui contract; b) depăşeşte limitele autorizării; c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfăşura alte activităţi (spre exemplu, cercetări ştiinţifice) sau de a efectua orice altă operaţiune într-un sistem informatic.

Aceasta înseamnă că nu va exista infracţiunea de acces ilegal în cazul în care există o autorizare prealabilă din partea proprietarului sistemului informatic sau din partea titularului de drept asupra sistemului informatic sau a unei părţi a acestuia (spre exemplu, pentru testarea sistemului în cauză). În cazul în care sistemul informatic permite acces public - deschis şi fără plată -, accesul va fi *cu drept*.

Elementul material în cazul primei variante agravate a infracţiunii constă în *accesul fără drept la un sistem informatic în scopul obţinerii de date informatice*. Accesul ilegal permite, în esenţă, realizarea tuturor atacurile periculoase împotriva datelor sau sistemelor informatice[717]; astfel de intruziuni pot crea impedimente pentru utilizatorii legitimi (autorizaţi) ai sistemelor informatice accesate legal, pot duce la accesarea[718], copierea[719] sau alterarea datelor informatice, comiterea de fraude[720], spionaj[721], şantaj[722] sau falsuri informatice,

---

717 Într-un caz interesant, J. J. Ancheta, folosind calculatoare pe care le controla pentru a transmite contaminanţi informatici pe Internet pentru a exploata calculatoare vulnerabile. El a direcţionat mii de calculatoare compromise către un canal Internet Relay Chat, unde acestea scanau pentru a depista alte calculatoare vulnerabile la infecţii similare, rămânând vulnerabile la acces neautorizat. El a obţinut şi bani din vânzarea de acces la aceste calculatoare (*botnets*) – vezi detalii în I. Vasiu, L. Vasiu, *Criminalitatea în cyberspaţiu*, op. cit.

718 Într-un astfel de caz, K. Kwak a plasat un program informatic pe calculatorul supervizorului său, care i-a permis acces în voie la respectivul calculator. El a folosit accesul neautorizat des pentru a accesa mesajele de poştă electronică ale supervizorului şi a monitoriza activităţile pe Internet ale acestuia; informaţiile astfel obţinute au fost comunicate şi altor colegi. Într-un alt caz, J. Jiang a instalat programe care capturează tastările la terminale situate la magazine Kinko, colectând, astfel, nume de utilizatori şi parole, folosite ulterior pentru a accesa conturi bancare aparţinând altor persoane – vezi detalii în I. Vasiu, L. Vasiu, *Criminalitatea în cyberspaţiu*, op. cit.

719 Într-un astfel de caz, de pe sisteme informatice ale Universităţii Stanford au fost copiate numere de Social Security, CV-uri, informaţii financiare şi numere de carduri de credit aparţinând unui număr de circa 10.000 de persoane.

720 Într-un astfel de caz, K. Flury a defraudat CitiBank în 2004 prin obţinerea de numere de carduri de debit şi PIN-uri, folosite subsecvente pentru crearea de carduri false şi retragerea de numerar de la ATM-uri, în total peste 384.000$ – vezi detalii în I. Vasiu, L. Vasiu, *Criminalitatea în cyberspaţiu*, op. cit.

721 Într-un astfel de caz, un maghiar a accesat ilegal sisteme informatice ale Ericsson Group şi a preluat informaţii senzitive - vezi http://www.thelocal.se/article.php?ID=1076&date=20050309. Într-un alt caz, M. şi R. Haephrati au fost arestaţi pentru că au folosit un cal troian informatic pentru a spiona sistemele informatice ale unor firme rivale – vezi detalii la http://www.guardian.co.uk/israel/Story/0,2763,1495716,00.html.

722 Vezi, spre exemplu, A. Salkever, *Cyber-Extortion: When data is held hostage*, BusinessWeek, August 22, 2000.

plasarea de contaminanţi informatici[723], obţinerea de parole de acces, sabotaj informatic[724], utilizarea fără plată a unor servicii etc.

Elementul material în cazul celei de-a doua variante agravate. Legiuitorul penal prevede, pentru varianta agravantă de la alin. 3, ca accesul ilegal să se realizeze prin folosirea unor *procedee, dispozitive sau programe* care trec peste măsurile de securitate care ar trebui să restricţioneze accesul ilegal, art. 35, lit. h) din Legea nr. 161/2003 definea măsurile de securitate ca fiind *folosirea unor proceduri, dispozitive sau programe informatice specializate* cu ajutorul cărora accesul la un sistem informatic este restricţionat sau interzis pentru anumite categorii de utilizatori. Prin urmare, legiuitorul noului Cod penal nu face decât să înlocuiască termenul generic "măsuri de securitate" cu definiţia acestuia din legea mai sus-menţionată.

Securitatea sistemelor informatice se referă la măsurile pe care o organizaţie sau persoană fizică le ia pentru a-şi proteja sistemele şi datele informatice (măsuri care vizează securitatea fizică a sistemelor informatice şi măsuri care vizează protejarea datelor şi programelor informatice). Încălcarea măsurilor de securitate îmbracă o diversitate de forme, o prezentare exhaustivă depăşind obiectivul acestei secţiuni[725].

Urmarea imediată constă într-o stare de pericol cu privire la siguranţa sistemului informatic şi/sau a resurselor sale prin încălcarea oricăreia dintre atributele descrise în cadrul secţiunii dedicate obiectului juridic: confidenţialitatea, integritatea şi disponibilitatea datelor sau sistemelor informatice.

Dacă scopul accesului neautorizat a fost obţinerea de date informatice, starea de pericol este dublată de atingerea adusă protecţiei datelor informatice stocate sau prelucrate de acesta. Încălcarea măsurilor de securitate determină o transformare efectivă adusă obiectului material al infracţiunii, anume al entităţilor materiale care compun sistemele informatice (calculatoare, reţele de calculatoare, echipament şi programe) sau datelor informatice vizate. Sub aspectul consecinţelor pe care acţiunea incriminată le are asupra valorii sociale ocrotite, urmarea este tocmai starea de pericol, de ameninţare, la adresa "domiciliului informatic".

Legătura de cauzalitate. Între activitatea incriminată săvârşită de făptuitor şi urmarea imediată trebuie să existe un raport de cauzalitate. Aceasta rezultă *ex re* în cazul accesului neautorizat în formă simplă, respectiv trebuie demonstrată

---

723 Într-un caz de acest tip, W. C. Shea, fost angajat ca programator şi manager al unei companii, în urma unor nemulţumiri la locul de muncă, a plasat o bombă informatică (*time bomb*) care ulterior a cauzat ştergerea şi modificarea unui număr mare de înregistrări financiare şi perturbarea sistemul informatic - vezi I. Vasiu, L. Vasiu, *Criminalitatea în cyberspaţiu*, op. cit.

724 Într-un astfel de caz, R. Fisher, după ce a părăsit locul de muncă în urma unor dispute pe probleme financiare, a cauzat întreruperea furnizării de servcii Internet în regiunea Vernal, Utah. Pentru a complica suplimentar eforturile de refacere a sistemului, infractorul a reprogramat punctele de acces – vezi detalii în I. Vasiu, L. Vasiu, *Criminalitatea în cyberspaţiu*, op. cit.; vezi şi S. Gaudin, *Net saboteur faces 41 months*, Network World, 4 martie 2002.

725 Pentru detalii, a se vedea Lucian Vasiu şi Ioana Vasiu, *Dissecting Computer Fraud: From Definitional Issues to a Taxonomy*, op. cit.; Lucian Vasiu şi Ioana Vasiu, *A Taxonomy of Malware use in the Perpetration of Computer-related Fraud*, Proceedings of the EICAR Conference, 2004.

forțarea măsurilor de securitate (parole, coduri de acces etc.), în cazul formei agravate. Cu toate că, în principiu, acest raport de cauzalitate ar trebui să fie ușor de identificat de organele judiciare, rezultând din materialitatea faptei, specificitatea mediului digital și ingeniozitatea celor care comit infracțiuni informatice face destul de dificilă această operațiune în practică.

b) Latura subiectivă presupune să existe un element subiectiv și cerința esențială.

Elementul subiectiv. Infracțiunea de acces ilegal se comite cu intenție directă sau indirectă[726].

Cerința esențială. În varianta de la alin. 2, legiuitorul prevede și o condiție esențială în legătură cu *scopul* realizării accesului fără drept: acela de a obține date informatice[727]. De regulă, făptuitorii caută date referitoare la utilizatori pentru a comite alte infracțiuni mai grave (fraude informatice, fals informatic, șantaj etc.).

Prin *date referitoare la utilizatori* se înțelege orice informație care poate conduce la identificarea unui utilizator, incluzând tipul de comunicație și serviciul folosit, adresa poștală, adresa geografică, numere de telefon sau alte numere de acces și modalitatea de plată a serviciului respectiv, precum și orice alte date care pot conduce la identificarea utilizatorului.

Forme, modalități, sancțiuni

A. Formele infracțiunii

a) Actele pregătitoare. Actele pregătitoare (procurarea sau realizarea de dispozitive vizând accesul ilegal) nu sunt pedepsite în cazul acestei infracțiuni, putând, însă, face obiectul unei alte infracțiuni, dacă sunt îndeplinite condițiile cerute de lege (infracțiunea incriminată în art. 365 din noul Cod penal: *Operațiuni ilegale cu dispozitive sau programe informatice*; spre exemplu, deținerea unui program de tip *malware* care permite accesul la un sistem informatic).

b) Tentativa este posibilă și se pedepsește conform art. 366 din noul Cod penal (acesta fiind conform art. 47 a Legii nr. 161/2003, sursa acestui articol din noul Cod penal).

c) Consumarea infracțiunii are loc în momentul în care se realizează urmarea imediată prevăzută de lege, adică intrarea în tot sau în parte a unui sistem informatic, în condițiile arătate de legiuitor, pentru fiecare dintre variante (simplă sau agravate).

---

[726] Într-un caz de acces ilegal, Gregory Aaron Herns a penetrat sistemul informatic al NASA la Goddard Space Flight Center in 2001, cauzând daune de US$200.000. Aparent, el voia să obțină spațiu pntru a stoca filme în format digital – vezi detalii la http://www.eweek.com/print article2/0,2533,a=141274,00.asp.

[727] Într-un caz din 2004, poliția din Tokyo a arestat două persoane pentru obținerea de date informatice privind clienții unei bănci și pentru incercarea de șantaj – vezi detalii la http://www.theregister.co.uk/2004/06/01/softbank_dat_leak/print.html. Într-un alt caz de acces ilegal pentru profit, Getloaded.com a accesat date informatice de pe sistemul Truckstop.com, care a realizat o afacere în legătură cu găsirea de încărcături (comenzi) pentru transporturile de distanțe mari astfel încât acestea să nu se deplaseze fără încărcătură la întoarcere – vezi detalii la http://caselaw.lp.findlaw.com/data2/circs/9th/0235856p.pdf.

BCU IASI CENTRAL UNIVERSITY LIBRARY

d) **Epuizarea** are loc în momentul comiterii ultimului act de acces ilegal. Infracţiunea este susceptibilă de a fi săvârşită în forma continuă (faptuitorul păstrează acces la sistemul informatic un timp îndelungat) sau continuată (prin penetrarea sistemelor informatice în mod repetat, întrerupând şi restabilind accesul ilegal).

Modalităţi

Modalităţile normative sunt cele arătate în textul de incriminare şi pot consta în următoarele activităţi: acces simplu, fără drept, accesul pentru obţinerea de date informatice, şi accesul realizat prin încălcarea măsurilor de securitate fizică sau pentru securitatea informaţiei stabilite de titular pentru restricţionarea accesului.

Modalitatea normativă simplă este cea arătată în primul alineat al art. 360 şi se referă la accesul simplu, fără drept.

Textul art. 360 cuprinde şi două **modalităţi normative agravate**. **Prima modalitate normativă agravată** prevăzută la art. 360 alin. (2) constă în fapta prevăzută în varianta simplă, dacă accesul fără drept s-a realizat în scopul obţinerii de date informatice. **A doua modalitate agravată** este cea prevăzută la art. 360 alin.(3) şi constă în fapta prevăzută în varianta simplă, dacă a fost săvârşită prin încălcarea *măsurilor de securitate* instituite legitim de titular pentru a restricţiona sau interzice accesul la sistemul informatic pentru anumite categorii. Procedurile, dispozitivele şi programele specializate prin care se realizează această interdicţie la sistemul respectiv vizează securitatea acestui sistem la una sau mai multe dintre următoarele componente: nivel fizic, operaţional, procedural, reţea şi aplicaţie.

Modalităţile faptice. Toate aceste modalităţi normative se pot prezenta într-o varietate de modalităţi de fapt (a se vedea explicaţiile date la concept şi caracterizare, respectiv latura obiectivă).

Sancţiuni

Faptele prevăzute la art. 360 se pedepsesc după cum urmează:

- Pentru forma simplă (alin. 1), pedeapsa este închisoarea de la 3 luni la 3 ani sau amendă;
- Pentru prima variantă agravantă (alin. 2), pedeapsa este închisoare de la 6 luni la 5 ani;
- Pentru a doua variantă agravantă (alin. 3), pedeapsa este închisoare de la 2 la 7 ani (mai puţin severă decât cea prevăzută în art. 42 din Legea nr. 161/2003, adică 3 la 12 ani, reducere semnificativă, nejustificată şi criticată la nivel internaţional).

Explicaţii complementare

A. Legătura cu alte infracţiuni: asemănări şi deosebiri. Asemănările sau deosebirile dintre accesul ilegal şi alte infracţiuni din codul penal sau din legi speciale se poate observa cu uşurinţă prin compararea textelor în discuţie. Având în vedere că valoarea centrală apărată prin prevederile din această reglementare este securitatea informatică, cu cele trei faţete fundamentale: integritatea, confidenţialitatea, disponibilitatea, este ceea ce distinge accesul ilegal la un sistem

BCU IASI / CENTRAL UNIVERSITY LIBRARY

informatic de alte infracţiuni care protejează alte atribute afectate prin atacurile informatice (spre exemplu, securitatea naţională, viaţa privată, secretul corespondenţei, securitatea tranzacţiilor electronice, securitatea şi inviolabilitatea sistemelor electronice de tranzacţionare, de depozitare sau de compensare-decontare în cadrul pieţei de capital, ocrotirea drepturilor de proprietate intelectuală, în special a drepturilor de autor, etc).

Astfel, accesul ilegal la un sistem informatic este *subsidiar* faţă de alte infracţiuni datorită caracterului lui de generalitate. Spre exemplu, infracţiunea încriminată de Legea nr. 297/2004[728] privind piaţa de capital - *accesul ilegal la un sistem electronic de tranzacţionare* este o variantă de specie a accesului ilegal la un sistem informatic. În acest caz, se va reţine infracţiunea încriminată de Legea nr. 297/2004 privind piaţa de capital- *accesul ilegal la un sistem electronic de tranzacţionare*, aplicându-se regula potrivit căreia generalul este subsidiar specialului.

Un alt exemplu este infracţiunea incriminată de art. 32, lit. q) din Legea nr. 535/2004 privind prevenirea şi combaterea terorismului, articol modificat şi completat de art. 159 din Legea 187/2012 pentru punerea în aplicare a Legii nr.286/2009, *fraude comise prin sisteme informatice şi mijloace de plată electronice şi infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice)*. Prin urmare, dacă se va realiza conţinutul infracţiunii de acces ilegal la un sistem informatic în condiţiile prevăzute de Legea nr. 535/2004 privind prevenirea şi combaterea terorismului (art. 32) vor fi incidente aceste prevederi, şi nu cele de faţă privitoare la infracţiunea de acces ilegal la un sistem informatic.

În multe cazuri din practică, accesul ilegal în sistemul informatic se face, de regulă, în scopul săvârşirii uneia sau mai multora dintre infracţiunile prevăzute în noul Cod penal, la Titlul II, Cap. IV, Fraude comise prin sisteme informatice şi mijloace de plată electronice, situaţie care justifică reţinerea unui concurs de conexitate etiologică în care accesul ilegal reprezintă mijlocul prin care realizarea de fraude informatice sau efectuarea de operaţiuni financiare în mod fraudulos, adică scopul, se realizează.

Infracţiunea de acces ilegal la un sistem informatic poate intra în concurs ideal în cazul în care are loc folosirea la bancomat, pentru retrageri de numerar sau orice alte operaţiuni financiare, a unui card falsificat sau a unuia real, fără consimţământul titularului său, cu infracţiunea de *Efectuare de operaţiuni financiare în mod fraudulos*, prevăzută art. 250 din noul Cod penal.

B. Aspecte procesuale. Pentru toate infracţiunile prevăzute în acest capitol, acţiunea penală se pune în mişcare din oficiu, iar urmărirea penală este efectuată de către organele de cercetare penală, sub supravegherea procurorului.

C. Precedente legislative şi situaţii tranzitorii

a) **Precedente legislative.** Infracţiunea de acces ilegal la un sistem informatic este în totalitate preluată (cu o mică modificare la o variantă

[728] Art. 279, alin.1, lit c). Se pedepseşte cu închisoare de la 6 luni la 5 ani şi interzicerea unor drepturi accesarea cu intenţie de către persoane neautorizate a sistemelor electronice de tranzacţionare, de depozitare sau de compensare-decontare (articol modificat prin art. 152, pct. 3 din Legea nr. 187/2012 pentru punerea în aplicare a Legii nr. 286/2009).

BCU IASI CENTRAL UNIVERSITY LIBRARY

agravantă, respectiv o detaliere a unui termen-cheie, și o reducere a sancțiunii pentru varianta agravată prevăzută la alin.3) din art. 42 din Legea nr 161/2003, a cărei sursă este Convenția europeană privind criminalitatea informatică (*Cybercrime Convention*).

b) **Situații tranzitorii.** Limitele de pedeapsă fiind mai reduse în noul Cod penal pentru varianta agravată prevăzută la alin. 3, în cazul succesiunii de legi penale în timp se va face aplicarea dispozițiilor din noul Cod penal.

Elemente de drept comparat

Cum sursa acestei incriminări este art. 2 din Convenția europeană privind criminalitatea informatică, Convenție care reprezintă, de fapt un adevărat tratat internațional în domeniu, fiind ratificată și de alte state din afara Europei, marea majoritate a statelor europene, dar și o serie de state non-europene, au prevederi similare în acest domeniu. Deși unele state au ales să criminalizeze „*hacking-ul* pur sau simplu", adică accesul ilegal la un sistem, urmând prevederile Convenției, alte state au prevăzut forme separate (agravate) pentru accesul ilegal: în *scopul obținerii de date informatice* (Slovacia și Portugalia) și prin *încălcarea măsurilor de securitate* (cazul prevederilor din Austria, Germania, Olanda, Lituania, Cipru, Olanda).

SUA, care au semnat și ratificat Convenția europeană împotriva criminalității informatice, au un text analog accesului ilegal la un sistem informatic, prevăzut în *Computer Fraud and Abuse Act* (CFAA). Această lege prevede ca ilegal, fie accesul intenționat și fără autorizare, fie cel care depășește (excede) autorizarea, pentru obținerea accesului la date protejate sau la un sistem informatic la care accesul este restricționat (a se vedea 18 U.S.C. § 1030).

Cu titlu de exemplu, enumerăm reglementările corespunzătoare, care au avut ca model acest articol 2 din Convenție, ale câtorva țări europene, care au preluat în legislația lor penală infracțiunea de acces ilegal la un sistem informatic, în deplin acord cu prevederea europeană: **Lituania**, în 198-1 Cod Penal; **Ungaria**, în art. 300 C (1) Cod Penal; **Olanda** în art. 138a Cod Penal; Italia, art. 615-*ter* Cod Penal; **Slovacia** în art. 247 (1) Cod Penal Act No. 300/2005 Co; **Portugalia**, în art. 7 L. nr. 109/ 91.

În prevederea **portugheză,** ca și în cea **română** și **slovacă** se prevede și un *scop special*, anume ca făptuitorul să urmărească prin accesul ilegal obținerea de date informatice (formă agravată). În **Codul penal francez**, în art. 323 - 1 Cod Penal se pedepsește infracțiunea de acces ilegal la un sistem informatic, acces la tot sau la o parte a sistemului informatic. Cerința esențială prevăzută de acest articol este ca accesul să fie fraudulos, spre exemplu dacă făptuitorul încalcă măsurile de securitate. De asemenea în acest articol este criminalizată și rămânerea într-un sistem informatic fără autorizare. La fel ca și Codul penal francez, **Codul penal italian**, în art. 615-*ter* pedepsește infracțiunea de acces ilegal la un sistem informatic, dar și rămânerea neautorizată în sistem. Același tip de prevedere există și în **Belgia.**

BCU IASI CENTRAL UNIVERSITY LIBRARY

În **Brazilia** în art. 154-B din legea penală în domeniu se prevede accesul ilegal la un sistem informatic, iar în **Mexic** este prevăzut în art. 211bis1 din Codul penal. Ambele texte sunt în acord deplin cu prevederea din art. 2 al Convenției europene împotriva criminalității informatice.

4.6.3 Interceptarea ilegală a unei transmisii de date informatice

Art. 361. (1) - Interceptarea, fără drept, a unei transmisii de date informatice care nu este publică și care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic se pedepsește cu închisoarea de la unu la 5 ani.
(2) - Cu aceeași pedeapsă se sancționează și interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic, ce conține date informatice care nu sunt publice.

Conținut legal și caracterizare

Această infracțiune nu are corespondent în vechiul Cod penal. Textul prevăzut de legiuitorul penal în noul Cod penal la art. 361, este preluat fără modificări din art. 43 al Legii nr. 161/2003, care, la rândul lui, are ca sursă textul propus de Convenția europeană în domeniul criminalității informatice, preluat, la rândul său, din Recomandarea 89/9 a Comitetului european pentru probleme criminale[729].

Formelor traditionale de spionaj li se adaugă o formă nouă: interceptarea ilegală a unei transmisii de date informatice. Intercepția de comunicații de date în tranzit constituie o violare gravă a caracterului privat al comunicațiilor, ca în cazul intercepției comunicațiilor prin viu grai sau telefon dintre indivizi[730]. Ne aflăm, deci, în prezența unei forme noi, moderne de ascultare, în special cea care constă în capturarea clandestină a emanațiilor electromangetice ale unui monitor (afișajul pe ecran al datelor - *emanations analysis*)[731].

Infracțiunea de interceptare ilegală a unei transmisii de date informatice este prevazută în art. 361 în două variante normative: prima (alin. 1) constă în interceptarea fără drept a unei transmisii de date informatice care nu este publică și care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se eféctuează în cadrul unui sistem informatic, respectiv (alin. 2) în interceptarea fără drept a unei emisii electromagnetice ce conține date informatice care nu sunt publice.

---

729 A se vedea Raportul explicativ la Convenția europeană în domeniul criminalității informatice – art. 3 Intercepția ilegală, paragraful 52.

730 Într-un caz, o femeie din statul Arizona a fost condamnată pentru interceptarea a peste 200 de mesaje de poștă electronică – vezi detalii la http://apnews.excite.com/article/20031019/D7U97UCG0.html.

731 A se vedea și textul Articolului 6 *Interceptarea ilegală* a Directivei Parlamentului European și a Consiliului privind atacurile împotriva sistemelor informatice și de abrogare a Deciziei-cadru 2005/222/JAI a Consiliului - SEC(2010) 1122 final și SEC(2010) 1123 final.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

Elemente preexistente

A. Obiectul juridic special constă în totalitatea relaţiilor sociale care privesc confidenţialitatea datelor informatice (dreptul la secretul datelor). Incriminarea interceptării ilegale în legislaţia penală face parte dintre măsurile (juridice şi tehnice) care vizează protejarea dreptului la secretul comunicaţiilor - dreptul la protecţia corespondenţei este statuat în art. 8 al Convenţiei Europene a drepturilor omului (consfinţit de art. 8 al Tratatului de la Lisabona, în care se introduce un drept separat privitor la protecţia vieţii private şi a datelor personale) - şi se aplică tuturor formelor de transmitere electronică a datelor: prin poştă electronică (*e-mail*), transfer de fişiere, fax etc. Textul art. 43 ocroteşte şi dreptul la o viaţă privată neperturbată şi la exclusivitatea comunicaţiilor de date.

Cu privire la prezentarea detaliată a conceptului de "confidenţialitate", valoare fundamentala a securităţii sistemelor şi datelor informatice facem trimitere la cele expuse în capitolul "Tehnologia informaţiilor şi comunicaţiilor".

B. Obiectul material al infracţiunii constă în suporturile materiale prin care se realizează comunicaţiile şi, mai ales, transferul de date pe calea telecomunicaţiilor publice sau private şi pe care sunt stocate datele informatice interceptate. Comunicaţiile se pot derula în interiorul aceluiaşi sistem informatic, între două calculatoare care transmit date unul către celalalt sau între un calculator şi o persoană (utilizator).

C. Subiecţii infracţiunii

a) **Subiect activ** al infracţiunii poate fi orice persoană (fizică sau juridică) care are capacitate penală, legea neprevăzând vreo cerinţă specială în legatură cu aceasta.
Participaţia penală este posibilă sub toate formele (complicitate, coautorat sau instigare).

b) **Subiect pasiv** este persoana al cărei drept la confidenţialitatea transmisilor de date a fost încălcat.

Structura juridică şi conţinutul constitutiv

Aceasta este alcătuită dintr-o **situaţie premisă** şi un **conţinut constitutiv** al infracţiunii.

A. Situaţia premisă. Această infracţiune nu poate exista în absenţa unui **sistem informatic** şi a unor **date informatice** asupra cărora făptuitorul să acţioneze în modalităţile prevăzute în textul de lege. De asemenea, această infracţiune nu poate exista în absenţa unor transmisii de date informatice sau emisii electromagnetice (care nu sunt publice), asupra cărora făptuitorul să acţioneze fraudulos în modalităţile prevăzute pentru realizarea scopului prevăzut în textul de lege şi bineînţeles, a unor sisteme informatice care le conţin sau din care provin or le sunt destinate.

Procesul de "transfer de date informatice" în cyberspaţiu cuprinde un spectru larg de furnizori. Prin urmare, este destul de facil de interceptat ilegal aceste transmisii, respectiv emisiile electromagnetice. Textul se referă la transmisiile de date care nu au caracter public; este vorba, în consecinţă de caracterul transmisiilor de date sau al emisiilor electromagnetice (ce se doreşte a fi

unele private, nepublice, confidenţiale, secrete între cei care transmit şi destinatarii legitimi), nu de caracterul datelor informatice sau emisiilor electromagnetice.

Acestea cuprind, în sens larg, aşa cum s-a urmărit de către leguitorul nostru în noul Cod Penal, urmând modelul european din Convenţie, toate comunicaţiile prin telefon, fax, e-mail sau transfer de fişiere. Alte state care au implementat intercepţia ilegală în legislaţia naţională nu precizează că transmisiile de date au caracter non-public, ci se referă la toate comunicaţiile (spre exemplu, legislaţia din Portugalia utilizează expresia: „toate comunicaţiile dintr-un sistem informatic"; cea din Bulgaria utilizează expresia: „mesaje"; cea din Statele Unite ale Americii: „orice comunicaţie prin fir, orală sau electronică"; legislaţia din Italia se aplică la toate tipurile de comunicaţii, publice sau nepublice).

A. Conţinutul constitutiv al infracţiunii

a) Latura obiectivă

Elementul material, în ambele variante, constă în acţiunea de *interceptare*.

Cerinţe esenţiale Pentru ca acţiunea de interceptare să facă obiectul elementului material al laturii obiective, trebuiesc îndeplinite următoarele cerinţe esenţiale:

- Interceptarea să aibă loc *fără drept* (cerinţă prevăzută pentru ambele variante normative). În sensul prezentului articol, acţionează fără drept persoana care se află în una dintre următoarele situaţii: nu este autorizată, în temeiul legii sau al unui contract; depăşeşte limitele autorizării; nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde.
- În cazul primei variante normative (alin. 1), *interceptarea* trebuie să privească o transmisie de date informatice care nu este publică şi care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic. În cazul celei de-a doua variante normative (alin. 2), interceptarea priveşte o emisie electromagnetică provenită dintr-un sistem informatic ce conţine date ce nu sunt publice.

Spre deosebire de Convenţia europenă privind criminalitatea informatică (vezi art. 3 – *Illegal interception*), legea română nu prevede în mod expres ca interceptarea să se realizeze prin mijloace tehnice, considerând, probabil, că nu are importanţă, din moment ce în mediul digital intercepţiile nu pot fi realizate decât folosind mijloace tehnice.

Unele legislaţii naţionale, cum este cea germană, prevăd această situaţie: interceptarea fără autorizare şi prin utilizarea de mijloace tehnice (Sec 202b St GB Data interception); la fel şi cea italiană care pedepseşte instalarea de dispozitive adaptate să intercepteze, să întrerupă, să obstrucţioneze comunicaţiile între sisteme informatice (art. 617- *quinquies* Cod penal).

Interceptarea prin mijloace tehnice se referă la ascultarea, monitorizarea sau supravegherea conţinutului comunicaţiilor, obţinerea conţinutului datelor fie direct, prin accesarea sistemului informatic, fie indirect recurgând la procedee clandestine.

Mijloacele tehnice includ dispozitive tehnice fixate pe liniile de transmisie, dispozitive care colectează/înregistrează comunicaţiile şi programe

informatice care facilitează intercepţia de date. Contaminanţii informatici (*malware*) pot fi utilizaţi pentru a intercepta transmisiile de date (spre exemplu, folosind un *keylogger*[732]).

Conceptul "nepublic" se referă, în prima variantă, la natura procesului transmisiei (comunicaţiilor) şi nu la natura datelor transmise. Datele pot fi disponibile public, dar părţile implicate în transmisie/comunicare doresc să facă acest lucru în condiţii private (de confidenţialitate) sau datele sunt ţinute secrete (protejate) până când, spre exemplu, accesarea acestora (serviciul) este plătit. Prin urmare, termenul 'nepublic' nu exclude *per se* comunicaţiile realizate prin reţele publice. Comunicaţiile de date ale angajaţilor, fie că sunt nu parte a derulării unor tranzacţii oficiale (legate de locul de muncă) şi care constituie transmisie de date care nu este publică sunt, de asemenea, protejate împotriva interceptării fără drept[733]. Comunicaţia sub forma transmisiei de date informatice poate să aibă loc într-un singur sistem informatic (spre exemplu, de la unitatea centrală spre imprimantă sau ecran), între două sisteme informatice, două calculatoare ori un calculator şi o persoană.

În varianta normativă de la alin. 2, legiuitorul incriminează *interceptarea fără drept a unei emisii electromagnetice*. "Emisia electromagnetică" este ceva obişnuit în cazul monitoarelor, în timp ce acestea sunt folosite pentru a se realiza diverse operaţii sau tranzacţii informatice. Astfel de emisii nu pot fi considerate *date* în sensul în care acestea sunt definite în art. 181 (2) noul Cod penal, orice reprezentare a unor fapte, informaţii sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic. Cu toate acestea, datele informatice, după cum sunt acestea definite în art. 181 (2) noul Cod penal, pot fi reconstituite, pornind de la emisiile electromagnetice.

Pentru ca intercepţia, în ambele variante, să fie ilegală în sensul art. 361 noul Cod penal, trebuie realizată *fără drept*. Actul va fi legitim dacă persoana care procedează la interceptare are dreptul de a dispune de datele comunicate, dacă ea acţionează la comandă sau cu autorizaţia participanţilor la comunicaţie, sau dacă, pe fondul unei dispoziţii legale specifice, supravegherea este autorizată în interesul securităţii naţionale ori pentru a permite autorităţilor să descopere infracţiuni care au fost comise.

Trebuie precizat că unele practici comerciale cum ar fi utilizarea de *cookies*[734] nu sunt considerate, de regulă, intercepţie fără drept. În ceea ce priveşte comunicaţiile cu caracter nepublic ale angajaţilor, în legislaţia fiecărui stat pot fi prevăzute excepţii în cazul cărora să fie permisă intercepţia unor astfel de

---

[732] Un "keylogger" este un program informatic care permite captarea tastărilor unui utilizator, ceea ce poate rezulta în obţinerea de parole de acces sau date financiare sau confidenţiale.

[733] A se vedea un astfel de caz la Curtea Europeană a drepturilor omului: EC HR – decizia în cazul *Halford v. UK*, 25 iunie 1997 20605/92. Spre deosebire de Europa, unde sunt protejate drepturile angajaţilor în legătură cu confidenţialitatea comunicaţiilor personale, în SUA situaţia este diferită: a se vedea *Regulating Internet privacy. The case for e-mail privacy rights*, p. 173 şi urm.

[734] Un *cookie* este un fişier text, stocat de browser-ul web pe calculatorul utilizatorului şi folosit pentru autentificare, stocare de informaţii sau preferinţe personale etc.

comunicații (spre exemplu, angajatorul poate realiza o asemenea activitate pentru a preveni divulgarea secretelor comerciale ale companiei).

Urmarea imediată constă în producerea pericolului pentru confifențialitatea transmisiilor de date informatice sau a emisiilor electromagnetice, pericol prevăzut de legiuitor în cele două variante, prin interceptarea fără drept a unei transmisii de date sau a emisiilor electromagnetice, în condițiile prevăzute de lege.

Legatura de cauzalitate. Între acțiunea de intercepție fără drept și urmarea imediată trebuie să existe un raport de cauzalitate, care rezultă din materialitatea faptei.

b) Latura subiectivă

Elementul subiectiv. Infracțiunea se comite cu intenție (directă sau indirectă)[735].

Mobilul și scopul săvârșirii infracțiunii nu constituie elemente componente al laturii subiective, însă stabilirea acestora poate contribui – în fiecare caz concret – la o justă individualizare a pedepsei.

Forme, modalități, sancțiuni

A. Formele infracțiunii

a) **Actele pregătitoare** sunt posibile, dar nu sunt pedepsite; ele pot face, însă, obiectul elementului material al infracțiunii prevăzute în art. 365 (spre exemplu, realizarea unui program informatic de tip *spyware* care permite interceptarea fără drept a unei transmisii de date informatice).
b) **Tentativa** este posibilă și se pedepsește conform art. 366 noul Cod penal.
c) **Consumarea infracțiunii** are loc în momentul producerii urmării imediate, adică crearea pericolului pentru confidențialitatea conținutului transmisiei de date informatice sau a emisiilor electromagnetice, in condițiile incriminate de legiuitor.
d) **Epuizarea infracțiunii** are loc în momentul comiterii ultimului act incriminat, în oricare din variantele normative. Infracțiunea se poate săvârși în forma continuată sau continuă.

B. Modalități

Modalitățile normative sunt cele arătate în textul de incriminare și pot consta în următoarele activități: *interceptarea, fără drept a unei transmisii de date informatice care nu este publică și intercepatrea fără drept a unei emisii electromagnetice.*

Modalitatea normativă simplă este cea arătată în primul alineat al art. 361 și se referă la, *interceptarea, fără drept a unei transmisii de date informatice care nu este publică*, iar în alin. (2) al art.361 este prevăzută **modalitatea asimilată**, care constă *în intercepatrea fără drept a unei emisii electromagnetice.*

Textul art. 361 nu cuprinde **modalități normative agravate**.

Modalități de fapt. Toate aceste modalități normative se pot prezenta într-o varietate de modalități de fapt (având în vedere tipurile extrem de variate de

[735] A se vedea și paragraful 58 din Raportul explicativ al Convenției europene privind criminalitatea informatică, unde se prevede în mod expres forma de vinovație intenția.

malware, în special programe malițioase de tip *spyware* și *sniffer* existente, tot atât de variate pot fi modalitățile de concretizare în practică utilizate de criminalii informatici).

C. **Sancțiuni**

Pentru faptele prevăzute în art. 361, în ambele variante, se prevede o pedeapsă cu închisoarea de la unu la 5 ani (mai puțin severă decât cea prevăzută în art. 43 al Legii nr 161/2003, adică 2 la 7 ani).

Explicații complementare

A. **Legătura cu alte infracțiuni: asemănări și deosebiri.**

Infracțiunea de interceptarea ilegală a unei transmisii de date informatice se aseamănă cu violarea corespondenței, atunci când aceasta din urmă se realizează prin modalitatea arătată la art. 302 alin. 2 noul Cod penal.

Infracțiunea de interceptarea ilegală a unei transmisii de date informatice, ca și celelalte infracțiuni contra siguranței și integrității sistemelor informatice este, cum am aratat deja, *subsidiară* față de alte infracțiuni datorită caracterului ei de generalitate (spre exemplu, infracțiunea incriminată de art. 32, lit.q) din Legea nr. 535/2004 privind prevenirea și combaterea terorismului, articol modificat și completat de art. 159 din Legea 187/2012 pentru punerea în aplicare a Legii nr.286/2009, *fraude comise prin sisteme informatice și mijloace de plată electronice și infracțiuni contra siguranței și integrității sistemelor și datelor informatice)*; prin urmare, dacă se va realiza conținutul infracțiunii de interceptarea ilegală a unei transmisii de date informatice în condițiile prevăzute de Legea nr. 535/2004 privind prevenirea și combaterea terorismului (art. 32) vor fi incidente aceste prevederi, și nu cele de față privitoare la infracțiunea de interceptarea ilegală a unei transmisii de date informatice.

Precum accesul ilegal la un sistem informatic, infracțiunea de interceptarea ilegală a unei transmisii de date informatice, este o „infracțiune mijloc", fiin comisă pentru a înlesni săvârșirea altora, intrând în concurs cu aceste infracțiuni (spre exemplu, cu fraudele comise prin sistemele informatice sau prin mijloacele de plată electronice).

B. **Aspecte procesuale.** Pentru infracțiunea de interceptarea ilegală a unei transmisii de date informatice, acțiunea penală se pune în mișcare din oficiu. iar urmărirea penală este efectuată de către organele de cercetare penală, sub supravegherea procurorului.

C. **Precedente legislative și situații tranzitorii**

a) **Precedente legislative.** Infracțiunea de interceptarea ilegală a unei transmisii de date informatice, este în totalitate preluată din art. 43 din Legea nr. 161/2003.

b) **Situații tranzitorii.** Limitele de pedeapsă fiind mai reduse în noul Cod penal, în cazul succesiunii de legi penale în timp se va face aplicarea dispozițiilor din noul Cod penal.

Elemente de drept comparat

Cum sursa acestei incriminări este art. 3 din Convenţia europeană privind criminalitatea informatică, marea majoritate a statelor europene au prevederi similare în acest domeniu. **Codul penal Italian** prevede infracţiunea de interceptare ilegală în art. 617-quarter şi art. 617-quinquies, art. 617-sexies şi art. 623 bis. **Codul penal austriac** prevede infracţiunea de interceptare ilegală în art. 119-119a. **Portugalia** prevede infracţiunea de interceptare ilegală în art. 8 din Legea nr. 109/1991. În **Germania**, secţiunea 202a Cod penal incriminează interceptarea ilegală a datelor informatice.

4.6.4 Alterarea integrităţii datelor informatice

Art. 362. Fapta de a modifica, şterge sau deteriora date informatice ori de a restricţiona accesul la aceste date, fără drept, se pedepseşte cu închisoarea de la unu la 5 ani.

Conţinut legal şi caracterizare

Datorită importanţei deosebite a datelor şi programelor informatice, a dependenţei organizaţiilor de procesarea corectă şi promptă a datelor informatice, alterarea integrităţii datelor informatice constituie un pericol major în lumea contemporană.

În vechiul Cod penal această infracţiune nu exista; infracţiunea este reprodusă în noul Cod penal, fără modificări, din Legea nr. 161/2003 (art. 44 al. 1).Scopul prevederii acestui text este acela de a asigura datelor şi programelor informatice o protecţie similară celei de care se bucură bunurile materiale împotriva activităţii intenţionate de provocare de daune.

Legiuitorul nostru penal, pornind de la textul art. 4 din Convenţia europeană privind criminalitatea informatică, a prevăzut în art. 44 al Legii nr. 161/2003 alterarea integrităţii datelor informatice. Astfel, în alin. 1 al art.44 era prevăzută fapta de a modifica, şterge sau deteriora date informatice ori de a restricţiona accesul la aceste date, fără drept, iar în alin.2 era incriminat transferul neautorizat de date dintr-un sistem informatic; această a doua variantă, în care se incriminează transferul neautorizat de date dintr-un mijloc de stocate a datelor informatice este acum prevăzută într-un articol separat de noul Cod penal, art. 364, **Transferul neautorizat de date informatice.**

În cazul infracţiunii de alterarea integrităţii datelor informatice, legiuitorul noului Cod penal, a simplificat încriminarea anterioară din art. 44 al Legii nr. 161/2003, prevăzând în art. 362 numai forma de bază a acesteia.

Elemente preexistente

A. Obiectul juridic special al infracţiunii constă în relaţiile sociale ce privesc integritatea şi funcţionarea sau utilizarea în condiţii optime a datelor sau programelor informatice.

B. Obiectul material al infracțiunii constă în suportul material pe care sunt stocate datele sau programele informatice (memorie cu acces aleator, disc dur, disc compact etc.).

C. Subiecții infracțiunii

a) **Subiect activ** poate fi orice persoană (fizică sau juridică) care are capacitate penală, textul neprevăzând nici o calitate specială pentru acesta.

Participația penală este posibilă sub toate formele.

b) **Subiect pasiv** este persoana fizică sau juridică având drepturi (de proprietate, de utilizare etc.) asupra datelor sau programelor informatice.

Structura și conținutul juridic al infracțiunii

Aceasta este alcătuită dintr-o **situație premisă** și un **conținut constitutiv** al infracțiunii.

A. Situația premisă. Această infracțiune nu poate exista în absența unor date informatice și, respectiv, a unor sisteme informatice care le conțin sau din care provin ori pentru care sunt destinate.

Pentru o aplicare corectă a textului de lege, începând cu Convenția europeană privind criminalitatea informatică și continuând cu alte mecanisme legale s-a încercat o definire cât mai precisă a conceptului-cheie "date informatice".

Cu privire la prezentarea detaliată a noțiunilor de „date informatice" și "sistem informatic" facem trimitere la cele expuse în capitolul "Tehnologia informațiilor și comunicațiilor".

B. Conținutul constitutiv al infracțiunii

A) Latura obiectivă

Elementul material al variante normative prevăzute de legiuitor constă în următoarele acțiuni ce implică efecte negative asupra stării datelor și/sau afectează capacitatea de funcționare sau procesare în maniera prevazută sau așteptată de persoana care dispune de sistemele informatice: *modificare*, *ștergere*, *deteriorare* sau *restricționarea* abuzivă a accesului la date informatice.

Ștergerea de date informatice este echivalentă cu distrugerea de obiecte materiale și include distrugerea suportului pe care acestea sunt stocate, supraimprimarea lor, modificarea tabelei de alocare a fișierelor etc.

Modificarea datelor informatice înseamnă alterarea în orice mod, schimbarea sau criptarea lor (aceste operațiuni pot fi realizate manual sau prin intermediul contaminanților informatici: viruși, viermi sau cai troieni informatici).

Deteriorarea datelor se referă la alterarea datelor sau programelor informatice ca urmare a unor acțiuni fizice sau logice ce rezultă în inutilizabilitea datelor sau sistemelor informatice.

Prin *restricționarea* accesului la date informatice se înțelege totalitatea actelor prin care datele nu mai sunt accesibile, într-un interval de timp rezonabil sau așteptat, persoanelor sau programelor informatice autorizate a le accesa sau procesa.

Activitățile menționate mai sus se pot realiza prin inserarea de programe malițioase: *viruşi, viermi, cai troieni* sau alte tipuri de *malware*.

Cerință esențială. Toate aceste activități menționate mai sus trebuie să fie realizate *fără drept*.

În sensul prezentului articol, acționează *fără drept* persoana care se află în una dintre următoarele situații: nu este autorizată, în temeiul legii sau al unui contract; depăşeşte limitele autorizării; nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a realiza alterarea datelor informatice într-o formă sau alta. În Codul nostru penal este singura cerință esențială cerută; în altele, spre exemplu, cea franceză, este prevăzut ca aceste activități de alterare să se "*realizeze fraudulos*", în timp ce alte legislații pedepsesc alterarea datelor dacă e "*serioasă*" sau "*gravă*".

Trebuie subliniat că activitățile obişnuite, inerente în proiectarea, realizarea şi testarea rețelelor informatice, reconfigurarea sistemelor de operare sau a aplicațiilor, autorizate de proprietar sau operator, nu constituie infracțiunea de alterare de date deoarece aceste activități se desfăşoară "*cu drept*". Modificarea traficului de date în scopul facilitării comunicațiilor anonime (spre exemplu, activitatea sistemelor informatice care retransmit anonim mesaje de poştă electronică), sau modificarea datelor în scopul securizării comunicațiilor (spre exemplu, criptarea datelor) trebuie, în principiu, considerate protecție legitimă, prin urmare realizate "cu drept".

Urmarea imediată constă în atingerea integrității datelor informatice prin una din activitățile incriminate în variantele prevăzute de legiuitor în art. 362 noul Cod penal.

Legatura de cauzalitate. Este necesar ca între acțiunile incriminate şi urmarea imediată să existe un raport de cauzalitate, care rezultă *per se*. Legiuitorul penal prevede în legatură cu aceste activități, o *cerință esențială*, în lipsa căreia acțiunile prezentate mai sus nu pot face obiectul elementului material al infracțiunii sub această formă—realizarea acțiunii *fără drept*. Persoanele care acționează fără a avea dreptul să o facă ori acționeaza contrar ori depăşesc autorizarea titularului vor fi considerate ca au acționat fără drept[736].

B) Latura subiectivă

Elementul subiectiv. Forma de vinovăție în cazul acestei infracțiuni este *intenția (directă sau indirectă)*. În majoritatea cazurilor, autorul doreşte producerea de daune; intenția de a scoate dintr-un asemenea act un profit ilicit nu este necesară şi nici tipică acestei forme de comportament infracțional. Totuşi, este posibil să existe o motivație indirectă lucrativă, cum ar fi dorința de a face rău unui concurent.

Daunele aduse integrității datelor informatice sunt adesea motivate de dorința de răzbunare a unui angajat sau fost angajat. Dorința de a atrage atenția,

---

[736] Un caz de alterare a integrității datelor a implicat un student din Texas care, aflându-se la domiciliu, a accesat propriile calificative academice, stocate pe un server al Universitatii, şi le-a "ameliorat". Într-un alt caz, un polițist din Ohio a accesat fişierele infracțiunilor rutiere pe un terminal şi a "eliminat" intrarea referitoare la sine (conducere periculoasă).

BCU IASI / CENTRAL UNIVERSITY LIBRARY

precum şi motivatiile ideologice sau politice apar de asemenea în conexiune cu această infracţiune.

Majoritatea legislaţiilor naţionale pedepsesc alterarea datelor dacă este săvârşită cu intenţie; există însă şi prevederi penale naţionale care pedepsesc neglijenţa care produce alterarea datelor.[737]

Mobilul şi scopul săvârşirii infracţiunii nu constituie elemente componente ale laturii subiective, însă stabilirea acestora poate contribui, în fiecare caz concret, la o justă individualizare a pedepsei.

Forme, modalităţi, sancţiuni

A. Formele infracţiunii

a) **Actele pregatitoare** sunt posibile, dar nu sunt incriminate. Actele pregătitoare (procurarea sau realizarea de dispozitive vizând alterarea datelor informatice) nu sunt pedepsite în cazul acestei infracţiuni, putând, însă, face obiectul unei alte infracţiuni, dacă sunt îndeplinite condiţiile cerute de lege (infracţiunea incriminată în art. 365 din noul Cod penal privind operaţiuni ilegale cu dispozitive sau programe informatice; spre exemplu, deţinerea unui program de tip *malware* care permite alterarea datelor informatice).

b) **Tentativa** este posibilă şi se pedepseste (conform art. 366 C. pen.).

c) **Consumarea infracţiunii** are loc în momentul producerii urmării imediate, adică a încălcării valorii ocrotite şi anume integritatea datelor. **Epuizarea infracţiunii** are loc în momentul comiterii ultimului act incriminat; infracţiunea se poate săvârşi şi în forma continuată.

B. Modalităţi

Modalităţile normative sunt cele arătate în textul de incriminare şi pot consta în următoarele activităţi: *introducere de date, modificarea de date ştergerea de date, restricţionarea accesului* la date *împiedicarea funcţionarii unui sistem informatic.*

Modalităţile de fapt. Toate aceste modalităţi normative se pot prezenta într-o varietate de modalităţi de fapt (a se vedea explicaţiile date la concept şi caracterizare, respectiv la latura obiectivă).

C. Sancţiuni

Pentru fapta prevăzută la art. 361 noul Cod penal pedeapsa este închisoarea de la unu la 5 ani.

Explicaţii complementare

A. Legătura cu alte infracţiuni. Infracţiunea de alterare a integrităţii datelor informatice, ca şi celelalte infracţiuni contra siguranţei şi integrităţii sistemelor informatice este, cum am aratat deja, *subsidiară* faţă de alte infracţiuni datorită caracterului ei de generalitate (spre exemplu, infracţiunea incriminată de art. 32, lit.q) din Legea nr. 535/2004 privind prevenirea şi combaterea terorismului, articol modificat şi completat de art. 159 din Legea nr. 187/2012 pentru punerea în

---

737 A se vedea art. 253 Codul Penal al Armeniei; art. 350B, Codul Penal al Olandei.

BOSA/CENTRAL UNIVERSITY LIBRARY

aplicare a Legii nr. 286/2009, *fraude comise prin sisteme informatice și mijloace de plată electronice și infracțiuni contra siguranței și integrității sistemelor și datelor informatice);* prin urmare, dacă se va realiza conținutul infracțiunii de Alterarea integrității datelor informatice în condițiile prevăzute de Legea nr. 535/2004 privind prevenirea și combaterea terorismului (art. 32) vor fi incidente aceste prevederi, și nu cele de față privitoare la infracțiunea de Alterarea integrității datelor informatice.

B. Aspecte procesuale. Pentru infracțiunea de Alterarea integrității datelor informatice, acțiunea penală se pune în mișcare din oficiu. iar urmărirea penală este efectuată de către organele de cercetare penală, sub supravegherea procurorului.

C. Precedente legislative și situații tranzitorii

a) **Precedente legislative.** Infracțiunea de alterarea integrității datelor informatice este în totalitate preluată (cu o mică modificare de sistematizare) din art. 44 alin. 1 al Legii nr. 161/2003, a cărei sursă este Convenția europeană privind criminalitatea informatică.

b) **Situații tranzitorii.** Limitele de pedeapsă fiind mai reduse în noul Cod penal decât cele din Legea nr. 161/2003, în cazul succesiunii de legi penale în timp se va face aplicarea dispozițiilor din noul Cod penal.

Elemente de drept comparat

Cum sursa acestei incriminări este art. 4 din Convenția europeană privind criminalitatea informatică, statelor europene au prevederi similare în acest domeniu. **Codul penal Italian** prevede, în art 635-bis și art. 635-ter, alterarea integrității datelor informatice. Acest articol din Codul penal este introdus prin Legea nr. 48/2008 și pedepsește mai grav interferența cu datele care sunt utilizate de statul italian sau de orice organ public, sau care are o utilitate publică. Prevederile se referă atât la alterarea datelor informatice, cât și a programelor.

Codul Penal Spaniol prevede, în art. 264-2, alterarea alterarea integrității datelor informatice. **Codul Penal Olandez** prevede în, art. 350a, alterarea alterarea integrității datelor informatice. În afară de pedepsirea alterării cu intenție este prevăzută și pedepsirea neglijenței în domeniu (art. 350b). **Codul Penal Slovac** prevede, în art. 247 (1) b, alterarea alterarea integrității datelor informatice.

4.6.5 Perturbarea funcționării sistemelor informatice

Art. 363. Fapta de a perturba grav, fără drept, funcționarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la date informatice, se pedepsește cu închisoarea de la 2 la 7 ani.

BCU IASI CENTRAL UNIVERSITY LIBRARY

Conținut legal și caracterizare

Această infracțiune nu are corespondent în vechiul Cod penal, sursa de inspirație pentru art. 363 noul Cod penal fiind art. 45 din Legea nr. 161/2003.

Sistemele informatice reprezintă un element esențial al interacțiunii politice, sociale și economice din Uniunea Europeană și la nivel global. Societatea este deja foarte dependentă de aceste sisteme, fenomenul fiind în creștere. Buna funcționare și securitatea acestor sisteme în Uniuna Europeană sunt vitale pentru dezvoltarea pieței interne și a unei economii competitive și inovatoare[738].

Perturbarea sistemelor informatice și ale sistemelor de telecomunicații poate avea consecințe chiar mai importante decât alterarea de date sau programe informatice. Deoarece sistemele informatice joacă un rol esențial în societatea modernă, protecția funcționării acestora prezintă un interes deosebit, atât pentru proprietarii sau operatorii sistemelor, cât și pentru societate în ansamblu. În general, împiedicarea funcționării corecte a unor sisteme informatice poate avea consecințe financiare sau operaționale majore[739].

Împiedicarea funcționării unor sisteme informatice critice (spre exemplu, a celor care controlează traficul urban, a unor rețele militare etc.) poate consecințe asupra unor categorii largi de persoane[740]. Pentru acest motiv, asemenea atacuri reprezintă o preocupare constantă la nivel global[741].

Atacurile cibernetice la scară largă pot provoca daune economice importante atât prin întreruperea funcționării sistemelor informatice și a comunicațiilor, cât și prin pierderea sau modificarea unor informații confidențiale importante din punct de vedere comercial sau a altor tipuri de date. În 12 decembrie 2010, Butyka Robert a accesat ilegal, prin încălcarea mijloacelor de securitate, mai multe servere aparținând NASA, producând perturbarea gravă a funcționării unui sistem informatic prin introducerea, modificarea și deteriorarea de date informatice și prin restricționarea accesului la aceste date, pagubele produse de infractor fiind de 300.000 de dolari, pentru repararea daunelor fiind necesari 200.000 de dolari[742]. Într-un alt caz, Răzvan Manole Cernacianu a atacat servere ale armatei SUA, ale NASA și ale Pentagonului, săvârșind infracțiunile de

---

738 Vezi Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013.

739 Vezi Nicole Perlroth și David E. Sanger, *Cyberattacks Seem Meant to Destroy, Not Just Disrupt*, NY Times, Mar. 28, 2013; Ronald J. Deibert, Rafal Rohozinski & Masashi Crete-Nishihata, *Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War*, Security Dialogue, 43, 2012.

740 Vezi Derek E. Bambauer, *Ghost in the network*, University of Pennsylvania Law Review 162 (5), 2014; Ronald J. Deibert, Rafal Rohozinski, Masashi Crete-Nishihata, *Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War*, Security Dialogue, 43, 2012; Marc Donner, *Cyberassault on Estonia*, IEEE Security & Privacy, 6, 2007.

741 A se vedea, spre exemplu, *Protecția infrastructurilor informatice critice: către un context global de securitate cibernetică* P7_TA(2012)0237, Rezoluția Parlamentului European din 12 iunie 2012 referitoare la protecția infrastructurilor critice de informație - realizări și etape următoare: către un context global de securitate cibernetică (2011/2284(INI)) (2013/C 332 E/03).

742 A se vedea detalii în Diana Biță, *Hackerul clujean acuzat că a spart serverele NASA a fost arestat*, 2011, la locația: http://www.romanialibera.ro/actualitate/eveniment/hackerul-clujean-acuzat-ca-a-spart-serverele-nasa-a-fost-arestat-244902.

acces ilegal la sisteme informatice, prin încălcarea măsurilor de securitate și în scopul obținerii de date informatice, transfer neautorizat de date dintr-un sistem informatic și perturbarea gravă a funcționării unui sistem informatic[743].

După cum se arată în Directiva europeană din 2013 privitoare la atacurile asupra sistemelor informatice, există dovezi în privința tendinței producerii unor atacuri la scară largă tot mai periculoase și recurente împotriva sistemelor informatice care, adesea, pot fi esențiale pentru state sau pentru funcții specifice din sectorul public sau privat. În paralel cu această tendință, se dezvoltă metode tot mai sofisticate, cum ar fi crearea și utilizarea așa-numitelor botnet-uri, care presupune etape succesive ale unei fapte penale, fiecare etapă prezentând un risc importante pentru interesele publice.

Deoarece pericolele ce rezultă în economie în caz de sabotaj informatic sunt considerate mai mari decat în cazul celor care rezultă în urma unor acțiuni de sabotaj economic, mai multe state ale lumii au prevazut în legislația lor penală texte de lege care incrimineaza *sabotajul informatic*. Textul art. 363 din noul Cod penal este preluat din textul art. 45 a Legii nr. 161/2003, care la rândul lui reproduce textul art. 5 al Convenției europene privind criminalitatea informatică (text similar, de altfel, cu cel al Recomandării 89/9 a Comitetului european pentru probleme criminale).

În art. 363 al noului Cod penal, se incriminează fapta de a perturba grav, fără drept, funcționarea unui sistem informatic prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la date informatice. Textul art. 363 este în deplin acord cu cerința fixată statelor membre de Directiva din 2013 privitoare la atacurile asupra sistemelor informatice.

Elemente preexistente

A. Obiectul infracțiunii

Obiectul juridic constă în relațiile sociale ce privesc dreptul proprietarului și/sau utilizatorului unui sistem informatic ori al unui sistem de telecomunicații de a fi în măsură să exploateze la potențialul real respectivul sistem.

B. Obiectul material constă în componentele de tip hardware ale sistemelor informatice atacate sau în suporturile materiale pe care se află stocate datele informatice care sunt ținta activităților criminale.

C. Subiecții infracțiunii

Subiect activ al infracțiunii poate fi orice persoană (fizică sau juridică) care are capacitate penală, cu precizarea pe care am făcut-o la infracțiunile prezentate anterior: de multe ori, autorii infracțiunilor sunt persoane care au cunoștinte relativ avansate în domeniul informatic sau sunt persoane care, prin natura serviciului lor, au sau au avut[744] acces la sisteme informatice.

Participația penală este posibilă în toate formele.

---

[743] http://www.romanialibera.ro/actualitate/eveniment/hackerul-tinkode-acuzat-de-diicot-si-fbi-ca-a-spart-servere-ale-nasa-si-pentagon-ramane-in-arest-252379.

[744] Vezi B. C. Nahrstadt, *Former Employee Sabotage? Invoke the Computer Fraud and Abuse Act*, Journal Of Internet Law, Feb., 2009.

BCU IASI CENTRAL UNIVERSITY LIBRARY

Subiect pasiv al infracţiunii este persoana care deţine sau utilizează legitim sistemul informatic care este ţinta atacului informatic incriminat.

Structura juridică şi conţinutul constitutiv al infracţiunii

Aceasta este alcătuită dintr-o **situaţie premisă** şi un **conţinut constitutiv** al infracţiunii.

A. Situaţia premisă

Această infracţiune nu poate exista în absenţa unui sistem informatic şi a unor date informatice asupra cărora făptuitorul să acţioneze fraudulos în modalităţile prevăzute pentru realizarea scopului prevăzut în textul de lege, adică perturbarea gravă a funcţionării sistemului informatic.

Cum am mai arătat şi la analiza articolelor precedente, aplicarea corectă a textului de lege de faţă este condiţionată de definirea precisă a termenilor cheie utilizaţi de legiuitor.

Cu privire la prezentarea detaliată a noţiunilor de "sistem informatic" şi „date informatice" facem trimitere la cele expuse în capitolul "Tehnologia informaţiilor şi comunicaţiilor".

B. Conţinutul constitutiv al infracţiunii

A) Latura obiectivă

Elementul material al infracţiunii se realizează prin *activitatea de perturbare* a funcţionării unui sistem informatic.

Cerinţe esenţiale. În legătură cu această activitate, legiuitorul prevede câteva *condiţii esenţiale* pentru existenţa infracţiunii sub această formă:

- Perturbarea să fie gravă,
- Să se facă fără drept,
- Ingerinţa cu consecinţe grave asupra funcţionării sistemului informatic să aibă loc prin introducerea, transmiterea, modificarea, ştergerea sau deteriorarea datelor informatice sau prin restricţionarea accesului la date informatice.

Deşi în Conventia europeană privind criminalitatea informatică se recomandă să se găsească şi să se prevadă un criteriu după care să se stabileasca ce înseamna "perturbare gravă", legiuitorul român lasă deschisă interpretarea, neprevăzând detalii. Experţii europeni care au lucrat la proiectul Convenţiei au propus o valoare a prejudiciului produs sau au considerat ca serioasă/gravă trimiterea de date către un sistem anume într-o asemenea formă, mărime sau frecvenţă încât să aibă un efect dăunător semnificativ asupra abilităţii proprietarului sau operatorului de a utiliza sistemul informatic sau de a putea comunica cu alte sisteme informatice (spre exemplu, prin intermediul unor atacuri de tip "refuz al serviciului", prin contaminarea sistemelor informatice[745] sau prin

[745] A se vedea definiţii şi o analiză a contaminanţilor informatici în L. Vasiu şi I. Vasiu, *A Taxonomy of Malware Use in the Perpetration of Computer-related Fraud*, op. cit.

folosirea sistemelor informatice pe post de *relay* pentru comunicaţii prin poşta electronică[746]).

Numai o analiză atentă, contextuală, care ţine seama de circumstanţe poate determina gravitatea perturbării unui sistem informatic. Perturbarea gravă trebuie să fie realizata *fără drept*, adică nu va exista în situaţii în care ingerinţa într-un sistem este permisă sau autorizată (spre exemplu, în situaţii de testare a securităţii sistemului informatic, de reconfigurare sau actualizare etc.).

Legiuitorul român a prevăzut următoarele tipuri de ingerinţe care pot da naştere la perturbări grave:

• *Introducerea* de date informatice, care priveşte atât introducerea de date exacte într-o maniera incorectă, eronată sau abuzivă, cât şi introducerea de date inexacte;

• *Transmiterea* datelor informatice, care se referă la comunicarea de date, ducând la supraîncărcarea sistemelor informatice;

• *Modificarea* datelor informatice, se referă la alterarea datelor, astfel încât acestea pot fi utilizate, dar procesarea lor va produce rezultate incorecte;

• *Ştergerea* datelor informatice, se referă la suprimarea datelor de pe suportul fizic pe care sunt stocate;

• *Deteriorarea* datelor informatice, se referă la alterarea negativă a datelor, astfel încât acestea nu mai pot fi utilizate;

• *Restricţionarea accesului* la date informatice, se referă la restricţionarea totală sau partială sau la întârzierea semnificativă a accesului la date, atunci când utilizatorul are nevoie de ele.

Acest tip de ingerinţe pot fi realizate cu ajutorul diverselor tipuri de *malware*. Potrivit rapoartelor periodice disponibile public, un număr impresionant de contaminanţi informatici sunt creaţi şi descoperiţi în fiecare an[747]. Aceste forme noi variază după obiectivele urmărite. Ca şi formele mai vechi de malware, noile forme de contaminanţi informatici pot fura bani, pot să indisponibilizeze sistemele informatice vitale, pot să ameninţe utilizatorii, etc.

Perturbarea gravă a sistemelor informatice se realizează destul de des în ultimii ani prin utilizarea de *botnets*[748]. Aceste atacuri pot afecta grav funcţionarea sistemelor informatice, rezultând în refuzul serviciului (*Distributed Denial of Service*)[749]. Alte exemple de acţiuni realizate de *botnet-uri*[750]: trimiterea de mesaje nesolicitate (*spam*): vezi cazurile Pushdo, care trimitea circa 10% din spam-ul la nivel global şi Waledac, care la un moment dat trimitea 1,5 milioane mesaje pe zi[751] sau Kelihos, care cuprindea 41.000 calculatoare infectate şi se consideră că

746 O asemenea activitate poate încetini semnificativ activitatea sistemelor informatice şi produce alte urmări nedorite pentru proprietarul sau operatorul sistemului informatic.

747 Vezi, spre exemplu, rapoartele trimestriale realizate de firme de specialitate, cum ar fi McAffee, Sophos, Symantec etc.

748 A se vedea în acest sens şi *T-CY Guidance Note #2 Provisions of the Budapest Convention covering botnets*, adopted by the 9th Plenary of the T-CY, 4-5 June 2013. A se vedea şi *Microsoft, the FBI, Europol and industry partners disrupt the notorious ZeroAccess botnet*.

749 Exemple de astfel de atacuri sunt *SynFlood*, *HTTPFlood*, *UDP Flood*, *smurf* sau *ping flood*.

750 Vezi ENISA, *Botnets: Detection, Measurement, Disinfection & Defence*, 2011.

751 Descrise în Cisco, op. cit., p. 4.

trimitea chiar 3,8 miliarde de mesaje nesolicitate pe zi pentru promovarea de produse farmaceutice, acţiuni bursiere şi pornografie infantilă (acest botnet era folosit şi pentru obţinerea de date personale)[752]; obţinerea de adrese de poştă electronică, numere de produs stocate în fişiere de configurare sau în regiştrii sistemului, parole, diverse documente, cod sursă, secrete comerciale, numere de cont sau carduri bancare[753]; instalarea de programe de tip *keylogger*, pentru a obţine ilegal date personale sau financiare (spre exemplu, cazul virusului informatic Coreflood); etc.

Există chiar servicii comerciale pentru lansarea de atacuri de refuz al serviciului distribuite împotriva unor site-uri web[754]. Autorii sunt foarte dificil de identificat, deoarece locaţia în care se află calculatoarele care alcătuiesc botnetul şi lansează atacul poate fi diferită de cea a autorului.

Mesajele de poştă electronică trimise în cantităţi masive pot, de asemenea, duce la pertubarea severă a sistemelor informatice. Într-un astfel de caz, *America Online v. National Health Care Discount*[755], au fost transmise 135 milioane de mesaje nesolicitate, ceea ce a dus la afectarea gravă a sistemelor informatice în cauză.

Urmarea imediată constă în producerea unui **rezultat** - o consecinţă a ingerinţei fără drept, perturbarea gravă a funcţionarii unui sistem informatic: *perturbarea gravă a funcţionării sistemului informatic*.

Legătura de cauzalitate. Între acţiunea incriminată şi urmarea imediată trebuie să existe un raport de cauzalitate. Expertiza informatică este esenţială în stabilirea existenţei acestui raport, aceasta putând răspunde şi la întrebarea vizând gravitatea perturbării şi dacă această consecinţă este urmarea acţiunii făptuitorului sau nu.

B) Latura subiectivă

Elementul subiectiv. Fapta de perturbare se comite cu intenţie directă sau indirectă. făptuitorul urmărind prin acţiunea sa perturbarea gravă a unui sistem informatic sau acceptând că o asemenea consecinţă se va produce în urma activităţii desfăşurate.

Mobilul şi scopul săvârşirii infracţiunii nu constituie elemente componente ale laturii subiective, însă stabilirea acestora poate contribui – în fiecare caz concret – la o justă individualizare a pedepsei.

---

[752] Vezi SANS, *NewsBites*, Vol. XIII, Iss. 78, 2011.

[753] Vezi cazul în care John Schiefer a infectat circa 250000 de calculatoare şi a folosit programe maliţioase (numite de el *spybot*) pentru a intercepta comunicaţii electronice pe Internet către www.paypal.com şi alte site-uri, ulterior, folosind informaţiile astfel obţinute, a accesat conturi bancare şi a efectuat cumpărături fără consimţământul sau ştiinţa titularilor – vezi cazul descris în US Department of Justice, *Computer security consultant charged with infecting up to a quarter million computers that were used to wiretap, engage in identity theft, defraud banks*, Release November 9, 2007.

[754] Vezi, spre exemplu, cazul IMDDOS Botnet, descris în Damballa, *The IMDDOS Botnet: Discovery and Analysis*, 2010.

[755] America Online v. National Health Care Discount, 174 F. Supp. 2d 890, 897 (N.D. Iowa 2001).

Forme. Modalități. Sancțiuni

A) Formele infracțiunii

a) **Actele pregătitoare** sunt posibile, dar nu se pedepsesc. sunt posibile, dar nu sunt incriminate. Actele pregătitoare (procurarea sau realizarea de dispozitive vizând perturbarea funcționării sistemului informatic) nu sunt pedepsite în cazul acestei infracțiuni, putând, însă, face obiectul unei alte infracțiuni, dacă sunt îndeplinite condițiile cerute de lege (infracțiunea incriminată în art. 365 din noul Cod penal: *operațiuni ilegale cu dispozitive sau programe informatice*; spre exemplu, deținerea unui program de tip malware care permite restricționarea accesului la datele informatice).

b) **Tentativa** este posibilă și se pedepsește conform art. 366 noul Cod penal.

c) **Consumarea infracțiunii** are loc în momentul producerii urmării imediate, adică a perturbării grave a funcționarii sistemului informatic.

d) **Epuizarea** are loc în momentul finalizării ultimului act incriminat de lege săvârșit de făptuitor.

B. Modalități

Modalitățile normative sunt cele arătate în textul de incriminare și pot consta în următoarele activități: *introducere de date*, *modificarea de date ștergerea de date, restricționarea accesului* la date *împiedicarea funcționarii unui sistem informatic.* Această formă tipică este prevăzută în art. 363 noul Cod penal.

Modalități faptice. Toate aceste modalități normative se pot prezenta într-o varietate de modalități de fapt (a se vedea explicațiile date la concept și caracterizare, precum și de la latura obiectivă).

C. Sancțiuni

Perturbarea gravă a funcționării unui sistem informatic se pedepsește cu închisoare de la 2 la 7 ani (în loc de 3 la 15 ani, așa cum era prevăzut de Legea nr. 161/2003). Legiuitorul noului Cod penal reduce și în acest caz pedeapsa, considerăm noi în mod nejustificat având în vedere gravitatea deosebită a acestei infracțiuni, "rudă apropiată" a terorismului (și a atacurilor masive asupra sistemelor vitale, care pot destabiliza chiar țări sau afecta grav activități importante la nivel global).

Explicații complementare

A. Legătura cu alte infracțiuni. Asemănări și deosebiri. Infracțiunea de perturbare gravă a funcționării unui sistem informatic ca și celelalte infracțiuni contra siguranței și integrității sistemelor informatice, este, cum am aratat deja, *subsidiară* față de alte infracțiuni datorită caracterului ei de generalitate (spre exemplu, infracțiunea incriminată de art. 32, lit. q) din Legea nr. 535/2004 privind prevenirea și combaterea terorismului, articol modificat și completat de art. 159 din Legea 187/2012 pentru punerea în aplicare a Legii nr.286/2009, *fraude comise prin sisteme informatice și mijloace de plată electronice și infracțiuni contra siguranței și integrității sistemelor și datelor informatice*). Prin urmare, dacă se va realiza conținutul infracțiunii de perturbare gravă a funcționării unui sistem

informatic în condițiile prevăzute de legea privind prevenirea și combaterea terorismului (art. 32) vor fi incidente aceste prevederi, și nu cele privitoare la infracțiunea de perturbare gravă a funcționării unui sistem informatic.

Menționăm faptul că perturbarea gravă a funcționării unui sistem informatic, dintre toate infracțiunile contra siguranței și integrității sistemelor informatice, este cea mai apropiată de cea de cyberterorism, fiind nevoie în cazurile din practică să se analizeze atent circumstanțele în care este comisă, motivația făptuitorilor și scopul urmărit pentru a le putea deosebi.

B. Aspecte procesuale. Pentru infracțiunea de perturbarea gravă a funcționării unui sistem informatic, acțiunea penală se pune în mișcare din oficiu. iar urmărirea penală este efectuată de către organele de cercetare penală, sub supravegherea procurorului.

C. Precedente legislative și situații tranzitorii

a) **Precedente legislative.** Infracțiunea de perturbarea gravă a funcționării unui sistem informatic este în totalitate preluată din art. 45 al Legii nr 161/2003, a cărei sursă este Convenția europeană privind criminalitatea informatică.

b) **Situații tranzitorii.** Limitele de pedeapsă fiind mai reduse în noul Cod penal, în cazul succesiunii de legi penale în timp se va face aplicarea dispozițiilor din noul Cod penal.

Elemente de drept comparat

Sursa acestei incriminări este art. 5 (*system interference*) din Convenția europeană privind criminalitatea informatică, marea majoritate a statelor europene având prevederi similare în acest domeniu. **Codul penal francez prevede** în art. 323-2 perturbarea funcționării sistemelor informatice (sau sabotajul informatic), Prevederea nu include cerința esențială ca perturbarea să fie" gravă", ci orice perturbare este pedepsită până la 5 ani închisoare sau amendă. **Codul penal austriac** prevede, în Secțiunea 126 B, perturbarea funcționării sistemelor informatice (sau sabotajul informatic), iar **Codul penal german** prevede, în secțiunea 303b, sabotajul informatic.

În **SUA**, perturbarea funcționării sistemelor informatice este prevăzută în 18 U.S.C. § 1030(a)(5)[756]. În anumite circumstanțe, asemenea cazuri pot fi clasificate drept terorism[757]. Dacă două sau mai multe persoane conspiră să cauzeze pertubarea unui sistme informatic al SUA, violând, astfel, 18 U.S.C. § 1030(a)(5), fiecare făptuitor poate fi acuzat de conspirație, conform 18 U.S.C. § 371.

În **Tailanda**, interferența cu date informatice este incriminata în Secțiunea 9, ca fiind distrugerea, modificarea sau amendarea ilegală a unor date informatice, în totalitate sau în parte. Interferența cu un sistem informatic este incriminata in Secțiunea 10, ca fiind acte care suspendă, întârzie, împiedică sau disrupt un sistem informatic, astfel încât acesta nu mai funcționează normal, în timp ce Secțiunea 11 incriminează transmiterea de date sau mesaje informatice unei alte persoane și

---

[756] Vezi o analiză detaliată a acestei infracțiuni în Ioana Vasiu și Lucian Vasiu, *Break on Through: An Analysis of Computer Damage Cases*, op. cit.

[757] *Id.*

mascarea unor asemenea transmisii de o manieră care împiedică funcționarea normală a sistemului afectat.

4.6.6 Transferul neautorizat de date

Art. 364. Transferul neautorizat de date dintr-un sistem informatic sau dintr-un mijloc de stocare a datelor informatice se pedepsește cu închisoarea de la unu la 5 ani.

Conținut legal și caracterizare

Această infracțiune nu are corespondent în vechiul Cod penal, fiind preluată din Legea nr. 161/2003 (art. 44 alin. 2 și 3). Datorită importanței deosebite a datelor și programelor informatice, a dependenței organizațiilor de procesarea corectă și promptă a datelor informatice, transferul neautorizat al datelor informatice dintr-un sistem informatic sau dintr-un mediu de stocare, constituie un pericol major în lumea contemporană.

Scopul prevederii acestui text este acela de a asigura datelor și programelor informatice o protecție similară celei de care se bucură bunurile materiale împotriva activității intenționate de provocare de daune, nu numai în situația activităților neautorizate de alterare, ci și de transfer neautorizat.

Legiuitorul nostru penal, pornind de la textul art. 4 din Convenția europeană privind criminalitatea informatică, dar mergând mai departe decât scopul acesteia, a prevăzut în art. 44 al Legii nr. 161/2003 alterarea integrității datelor informatice în mai multe variante normative. Astfel, în alin. 1, era prevăzută fapta de a modifica, șterge sau deteriora date informatice ori de a restricționa accesul la aceste date, fără drept; în alin. 2 este incriminat transferul neautorizat de date dintr-un sistem informatic; în alin. 3 se incrimina transferul neautorizat de date dintr-un mijloc de stocate a datelor informatice.

În cazul acestei infracțiuni prevăzută la art. 4 al Convenției Europene privind criminalitatea informatică, legiuitorul noului Cod penal, a preferat o altă configurație, prevăzând forma de bază a acesteia în art. 362, iar celelalte două, transformate într-o infracțiune nouă, la art. 364, text supus analizei noastre.

Elemente preexistente

A. Obiectul juridic special al infracțiunii constă în relațiile sociale ce privesc integritatea și funcționarea sau utilizarea în condiții optime a datelor informatice (inclusiv a programelor informatice).

B. Obiectul material al infracțiunii constă în suportul material pe care sunt stocate datele sau programele informatice (stick de memorie, memorie cu acces aleator, disc dur, disc compact etc.), date sau programme transferate neautorizat.

C. Subiecții infracțiunii

a) **Subiect activ** poate fi orice persoană (fizică sau juridică) cu capacitate penală, textul de lege neprevăzând vreo calitate specială pentru acesta. **Participația penală** este posibilă sub toate formele.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

b) **Subiect pasiv** este persoana fizică sau juridică având drepturi (de proprietate, de utilizare etc.) asupra datelor sau programelor informatice.

Structura şi conţinutul juridic al infracţiunii

Aceasta este alcătuită dintr-o **situaţie premisă** şi un **conţinut constitutiv** al infracţiunii.

Situaţia premisă. Această infracţiune nu poate exista în absenţa unor **date informatice** aflate într-un sistem informatic sau într-un **mediu de stocare**, asupra cărora făptuitorul să acţioneze fraudulos în modalitatea prevăzută pentru realizarea scopului prevăzut în textul de lege, adică aceea de a *transfera neautorizat aceste date*.

Cu privire la prezentarea detaliată a noţiunilor de "sistem informatic" şi "date informatice" facem trimitere la cele expuse în capitolul "Tehnologia informaţiilor şi comunicaţiilor". Prin "mediu de stocare" se înţelege materialul pe care datele sunt stocate[758]. Deoarece memoria calculatoarelor poate păstra numai cantităţi mici de date şi programe, şi deoarece RAM (memoria cu acces aleator) este o memorie volatilă, este necesară utilizarea unor periferice pentru stocarea datelor. Cele mai importante medii de stocare sunt banda magnetică, discul magnetic, discul compact şi videodiscul.

Conţinutul constitutiv al infracţiunii

A) Latura obiectivă cuprinde elementul material, cerinţe esenţiale şi urmarea imediată.

Elementul material al variantei prevăzute de legiuitorul penal constă în acţiunea de *transfer neautorizat de date*.

Prin "*transfer*" se înţelege transmiterea sau copierea de date informatice de pe un suport fizic pe un altul (spre exemplu, de pe un disc dur pe un disc compact etc.). Transferul poate implica şi distrugerea datelor la locaţia originala (de unde se face tranmisia).

Cerinţa esenţială. În legatură cu acţiunea de transfer, legiuitorul prevede condiţia esenţială de a fi *neautorizat* - persoana care are drepturi asupra datelor nu a permis transferul, sau l-a permis, dar într-o modalitate diferită, autorul transferului depăşind sfera sau nivelul de autorizare (spre exemplu, în situaţia în care există dreptul de a transfera date informatice, dar numai de un anumit tip, către anumite entităţi sau pentru o anumită perioadă de timp).

Legiuitorul prevede adiţional o **condiţie esenţială** pentru fiecare dintre variantele alternative inserate în acest articol :

• În cazul primei variante prevăzute, transferul neautorizat de date trebuie să se facă dintr-un *sistem informatic*. Prin "sistem informatic", în sensul art. 181 (alin. 1) din nou Cod penal se înţelege *orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie functională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, folosind programe informatice*. Am

---

[758] Pentru detalierea fiecărui mediu de stocare, a se vedea, I. Vasiu, L.Vasiu, *Informatica juridică şi drept informatic 2009*, op. cit., p. 30-32.

BCU CLUJ / CENTRAL UNIVERSITY LIBRARY

prezentat mai sus la secţiunea consacrată premisei juridice definiţia dată sistemului informatic de Directiva din 2013.

• În cazul celei de-a doua variante prevăzute, transferul neautorizat de date se realizează dintr-un *mijloc de stocare* a datelor informatice (spre exemplu, stick de memorie, disc sau bandă magnetică, disc compact etc.).

Urmarea imediată constă în atingerea integrităţii, confidenţialităţii şi/sau disponibilităţii datelor informatice prin una din activităţile incriminate în variantele prevăzute de legiuitor în art. 364.

Legătura de cauzalitate. Este necesar ca între acţiunile incriminate şi urmarea imediată să existe un raport de cauzalitate, care rezultă *per se*.

B) Latura subiectivă

Elementul subiectiv. Vinovăţia la această infracţiune se prezintă sub forma intenţiei: *directă* sau *indirectă*.

Mobilul şi scopul săvârşirii infracţiunii nu constituie elemente componente ale laturii subiective, însă stabilirea acestora poate contribui – în fiecare caz concret – la o justă individualizare a pedepsei.

Forme, modalităţi, sancţiuni

A. Forme

a) **Actele pregatitoare** sunt posibile, dar nu sunt incriminate. Actele pregătitoare (procurarea sau realizarea de dispozitive vizând transferul neautorizat de date informatice) nu sunt pedepsite în cazul acestei infracţiuni, putând, însă, face obiectul unei alte infracţiuni, dacă sunt îndeplinite condiţiile cerute de lege (infracţiunea incriminată în art. 365 din noul Cod penal privind operaţiuni ilegale cu dispozitive sau programe informatice; spre exemplu, deţinerea unui program de tip malware care permite transferul neautorizat de date informatice).

b) **Tentativa** este posibilă şi se pedepseste (conform art. 366 C.pen.)

c) **Consumarea infracţiunii** are loc în momentul producerii urmării imediate, adică a punerii în pericol a valorii ocrotite (securitatea datelor informatice, prin activitatea de transfer neautorizat).

Epuizarea infracţiunii are loc în momentul comiterii ultimului act incriminat; infracţiunea se poate săvârşi şi în forma continuată.

B. Modalităţi

Modalităţile normative sunt cele arătate în textul de incriminare şi pot consta în următoarele activităţi: *transferul neautorizat de date dintr-un sistem informatic sau transferul neautorizat de date dintr-un mediu de stocare.*

Modalităţile faptice. Toate aceste modalităţi normative se pot prezenta într-o varietate de modalităţi de fapt.

C. Sancţiuni

Transferul neautorizat de date informatice dintr-un sistem informatic sau dintr-un mediu de stocare este pedepsit de legiuitorul noului cod penal cu închisoare de la unu la 5 ani.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

Explicații complementare

A. Legătura cu alte infracțiuni. Infracțiunea de transfer neautorizat de date informatice ca și celelalte infracțiuni contra siguranței și integrității sistemelor informatice este, cum am aratat deja, *subsidiară* față de alte nfracțiuni datorită caracterului ei de generalitate (spre exemplu, infracțiunea incriminată de art. 32, lit.q) din Legea nr. 535/2004 privind prevenirea și combaterea terorismului, articol modificat și completat de art. 159 din Legea 187/2012 pentru punerea în aplicare a Legii nr. 286/2009, *fraude comise prin sisteme informatice și mijloace de plată electronice și infracțiuni contra siguranței și integrității sistemelor și datelor informatice)*; prin urmare, dacă se va realiza conținutul infracțiunii de transfer neautorizat de date informatice în condițiile prevăzute de legea privind prevenirea și combaterea terorismului (art. 32) vor fi incidente aceste prevederi, și nu cele de față privitoare la infracțiunea de transfer neautorizat de date informatice.

B. Aspecte procesuale. Pentru infracțiunea de transfer neautorizat de date informatice, acțiunea penală se pune în mișcare din oficiu, iar urmărirea penală este efectuată de către organele de cercetare penală, sub supravegherea procurorului.

C. Precedente legislative și situații tranzitorii

a) Precedente legislative. Infracțiunea de transfer neautorizat de date informatice este în totalitate preluată din Legea nr 161/2003, a cărei sursă este Convenția europeană privind criminalitatea informatică (cu o mică modificare de sistematizare, respectiv despărțirea articolului-sursă din legea specială în două articole în noul Cod penal, din art. 44, alin. 2 și 3).

b) Situații tranzitorii. Limitele de pedeapsă fiind mai reduse în noul Cod penal, în cazul succesiunii de legi penale în timp se va face aplicarea dispozițiilor din noul Cod penal.

4.6.7 Operațiuni ilegale cu dispozitive sau programe informatice

---

Art. 365. (1) Fapta persoanei care, fără drept, produce, importă, distribuie sau pune la dispoziție sub orice formă:

a. dispozitive sau programe informatice concepute sau adaptate în scopul comiterii uneia dintre infracțiunile prevăzute în art. 360-364;

b. parole, coduri de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic, în scopul săvârșirii uneia dintre infracțiunile prevăzute în art. 360-364, se pedepsește cu închisoare de la 6 luni la 3 ani sau cu amendă.

(2) Deținerea, fără drept, a unui dispozitiv, a unui program informatic, a unei parole, a unui cod de acces sau a altor date informatice dintre cele prevăzute în alin. (1), în scopul săvârșirii uneia dintre infracțiunile prevăzute în art. 360-364, se pedepsește cu închisoare de la 3 luni la 2 ani sau cu amendă.

BCU ASE CENTRAL UNIVERSITY LIBRARY

Conținut legal și caracterizare

Această infracțiune nu are corespondent în vechiul Cod penal, fiind reprodusă de legiuitorul noului Cod penal din art. 46 al Legii nr.161/2003. Textul prevăzut de legiuitorul nostru în art. 365 noul Cod penal este similar art. 6 din Convenția europeană împotriva criminalității informatice (*Misuse of devices*). Acest text este, de asemenea, în deplin acord cu ultimele obligații prevăzute pentru statele membre în Directiva din 2013, privind atacurile asupra sistemelor informatice.

Textul de la art. 365 se constituie în incriminarea unor acte ilegale specifice, având ca obiect dispozitive sau coduri de acces, utilizate în scopul comiterii infracțiunilor prevăzute în art. 360-364, după cum urmează:

• Prima variantă normativă (alin. 1, lit. a), constă în fapta de a produce, vinde, importa, distribui sau de a pune la dispoziție sub orice altă formă, fără drept, a unui dispozitiv sau program informatic conceput sau adaptat în scopul săvârșirii uneia din infracțiunile prevăzute în art. 360-364;

• A doua variantă normativă (alin. 1, lit.b), constă în fapta de a produce, vinde, importa, distribui sau de a pune la dispoziție sub orice formă, fără drept, a unei parole, cod de acces sau alte date care permit accesul total sau parțial la un sistem informatic în scopul săvârșirii uneia din infracțiunile prevăzute în art. 360-364;

• A treia variantă normativă (alin. 2), care este sancționată mai puțin sever, constă în deținerea, fără drept, a unui dispozitiv, program informatic parolă, cod de acces sau date dintre cele prevăzute in alin. 1 în scopul săvârșirii uneia din infracțiunile prevăzute in art. 360-364.

Spre exemplu, o persoană care produce dispozitive USB care conțin contaminanți informatici care distrug date când dispozitivul este conectat la un calculator comite infracțiunea de operațiuni ilegale cu dispozitive sau programe informatice în concurs cu alterarea integrității datelor informatice[759]. Phishing-ul poate fi inclus în această categorie; în SUA, spre exemplu, cazurile de acest tip sunt urmărite penal conform 18 USC § 1029, fiind considerat un dispozitiv informatic care permite accesul ilegal la sisteme informatice.

Într-un caz din anul 2011, un grup de persoane a fost trimis în judecată pentru utilizarea și comercializarea, directă și prin intermediul Internet, de produse informatice destinate interceptării ilegale de comunicații și transmisii de date realizate prin intermediul terminalelor de telefonie mobilă[760]. Într-un alt caz, George P., alias "Bush", a fost trimis în judecată pentru operațiuni ilegale cu dispozitive sau programe informatice și condamnat la cinci ani de închisoare[761].

Conform Directivei din 2013 a Parlamentului European și a Consiliului privind atacurile împotriva sistemelor informatice și de abrogare a Deciziei-cadru 2005/222/JAI a Consiliului (SEC(2010) 1122 final, SEC(2010) 1123 final), în art.

759 Vezi ITU, *Understanding cybercrime: A guide for developing countries*, 2009.

760 A se vedea detalii la locația: http://alba24.ro/dosarul-spionii-din-dormitor-inculpati-achitati-de-curtea-de-apel-alba-iulia-decizia-nu-este-definitiva-293429.html

761 A se vedea detalii la locația: http://www.tribunalulvrancea.ro/downloads/sintezapresei/sinteza%2005.04%20-%2011.04.pdf.

7 *Instrumentele utilizate pentru comiterea faptelor penale*, se solicită adoptarea de măsuri necesare pentru a garanta că se pedepsesc ca infracţiune atunci când sunt comise intenţionat şi fără a avea dreptul, în vederea comiterii uneia dintre faptele penale menţionate la articolele 3-6 prevăzute în această Directivă (adică oricare din infracţiunile de: Accesarea ilegală a sistemelor informatice, Interceptarea ilegală, Alterarea integrităţii datelor informatice şi Perturbarea funcţionării sistemelor informatice), "producerea, vânzarea, achiziţionarea în vederea utilizării, importul, deţinerea, distribuirea sau punerea la dispoziţie în alt mod a:

(a) unui dispozitiv, inclusiv program de calculator, conceput sau adaptat în principal în scopul comiterii oricăreia dintre faptele menţionate la articolele 3-6 (adică Accesarea ilegală a sistemelor informatice, Interceptarea ilegală, Alterarea integrităţii datelor informatice şi Perturbarea funcţionării sistemelor informatice);

(b) unei parole de calculator, unui cod de acces sau a unor date similare, prin care un întreg sistem informatic sau orice parte a acestuia poate fi accesat(ă)".

Directiva prevede, în Art. 11, răspunderea persoanelor juridice: "Statele membre adoptă măsurile necesare pentru a se asigura că persoanele juridice pot fi trase la răspundere pentru oricare dintre faptele prevăzute la articolele 3-8, comise spre folosul lor de către orice persoană, acţionând fie în nume propriu, fie ca parte a unui organism al persoanei juridice şi având o funcţie de conducere în cadrul persoanei juridice, în temeiul:

(a) unei împuterniciri din partea persoanei juridice;
(b) unei prerogative de a lua decizii în numele persoanei juridice;
(c) unei prerogative de a exercita controlul în cadrul persoanei juridice".

Tot în Art. 11, se solicită ca statele membre să adopte măsurile necesare pentru a garanta că se poate antrena răspunderea juridică a persoanelor juridice în cazul în care, "ca urmare a nesupravegherii sau neexercitării controlului, imputabile unei persoane menţionate la alin. (1), a fost posibilă săvârşirea, de către o persoană aflată în subordine, a oricăreia dintre faptele menţionate la articolele 3-8, în folosul acelei persoane juridice" (desigur, răspunderea persoanelor juridice în temeiul alineatelor (1) şi (2) nu exclude procedurile penale îndreptate împotriva persoanelor fizice care sunt autori sau complici la oricare din faptele prevăzute la articolele 3-8 din această Directivă).

De vreme ce, pentru comiterea infracţiunilor mai sus menţionate, este nevoie, cel mai adesea, de posesia unor mijloace de acces sau alte mijloace, există, prin urmare, o puternică pornire în a le achiziţiona pentru scopuri criminale, ceea ce poate duce la crearea unei periculoase "pieţe negre" a contaminanţilor informatici (adevătate "cutii cu scule ale criminalilor informatici")[762]. Pentru a combate efectiv acest pericol, legislaţia penală trebuie să interzică aceste acte periculoase de la sursă, precedând comiterea infracţiunilor prevazute în art. 360-364 noul Cod penal.

---

762 Vezi Thomas J. Holt, *Examining the Forces Shaping Cybercrime Markets Online*, Social Science Computer Review, 31, 2013.

Această incriminare este clădită pe dezvoltările ce au avut loc în domeniu la nivel european (privind protecţia legală a serviciilor bazate pe/sau constând în acces condiţionat) şi dispoziţiile relevante existente în unele ţări[763].

Elemente preexistente

A. Obiectul juridic special constă în relaţiile sociale ce privesc drepturile proprietarilor sau deţinătorilor de date şi sisteme informatice la protecţia integrităţii, confidenţialităţii şi disponibilităţii acestora. Pentru a evita repetarea, cu privire la prezentarea detaliată a celor trei componente fundamentale a securităţii sistemelor şi datelor informatice: integritate, confidenţialitate şi disponibilitate, facem trimitere la cele expuse în capitolul "Tehnologia informaţiilor şi comunicaţiilor".

B. Obiectul material al infracţiunii constă în entităţile materiale în care sunt exprimate mijloacele puse în circulaţie sau deţinute în scopul comiterii infracţiunilor prevăzute în art. 360-364 (în cazul în care acestea sunt reprezentate de programe informatice sau coduri de acces, obiectul material va consta în suporturile materiale pe care acestea sunt păstrate).

Trebuie mentionat că, în cazul activităţii criminale realizate prin producerea acestor mijloace, obiectul material va consta în entităţile materiale asupra cărora se acţionează pentru a le confecţiona şi nu în aceste mijooace, care vor constitui rezultat (produs) al infracţiunii.

C. Subiecţii infracţiunii

a) **Subiect activ** al infracţiunii poate fi orice persoană (fizică sau juridică) care are capacitate penală, legea necerând nici o condiţie specială pentru autorul infracţiunii; de regulă, însă, actele ilegale care fac obiectul acestei infracţiuni sunt comise de persoane cu cunoştinţe de specialitate avansate, mai ales în variante de producere a acestor mijloace.

   Participaţia penală este posibilă sub toate formele.

b) **Subiect pasiv** al infracţiunii este persoana ale cărei drepturi la integritatea, confidenţialitatea şi disponibilitatea datelor şi/sau sistemelor informatice sunt puse în pericol prin activităţile incriminate în acest text de lege.

Structura şi conţinutul juridic al infracţiunii

A. Situaţia premisă

Infracţiunea de Operaţiuni ilegale cu dispozitive sau programme informatice fiind o infracţiune mijloc, trebuie să fie de natură a contribui la săvârşirea uneia sau unora din infracţiunile menţionate în textul de lege, infracţiuni prevăzute la art. 360-365 noul Cod penal: Accesarea ilegală a sistemelor informatice, Interceptarea ilegală, Alterarea integrităţii datelor informatice,

---

[763] O abordare similara a existat în ceea ce priveste Convenţia de la Geneva din 1929, privind contrafacerea de monedă – a se vedea Raportul explicativ al Convenţiei europene privind criminalitatea informatică, art. 6.

Perturbarea funcţionării sistemelor informatice şi Transferul neautorizat de date informatice.

Situaţia premisă constă în existenţa unei varietăţi de *instrumente, programe informatice sau dispozitive*, utilizate într-o varietate de moduri la săvârşirea infracţiunilor mai sus menţionate. Aceste instrumente utilizate la comiterea infracţiunilor informatice *(malware)* sunt în mod normal create sau adaptate în principal pentru a comite infracţiunile prevăzute la art.360-364 (Accesarea ilegală a sistemelor informatice, Interceptarea ilegală, Alterarea integrităţii datelor informatice şi Perturbarea funcţionării sistemelor informatice).

B. Conţinutul constitutiv al infracţiunii

A) Latura obiectivă

Elementul material constă, în cazul variantelor prevăzute în alin. 1 şi 2, în următoarele acţiuni: producere, vânzare, import, distribuţie, punere la dispoziţie sub orice altă formă.

Cerinţe esenţiale. În legătură cu aceste acţiuni sunt prevăzute *cerinţe esenţiale* în cazul fiecărei variante normative:

• Acţiunile incriminate să se realizeze *fără drept* (cerinţa esentială prevăzută de legiuitor în toate variantele normative);

• Acţiunile incriminate în prima variantă, la alin. 1, lit. a) şi comise *fără drept* trebuie să privească un *dispozitiv sau program informatic* conceput sau adaptat în scopul săvârşirii uneia din infracţiunile prevăzute în art. 360-364 noul Cod penal;

• Acţiunile incriminate în varianta de la alin. 1, lit. b), comise fără drept, trebuie să privească *o parolă, un cod de acces sau alte asemenea date informatice* care permit accesul total sau parţial la un sistem informatic în scopul săvârşirii uneia din infracţiunile prevăzute în art. 360-364 Noul cod penal.

"Distribuirea" la care face referire textul de lege înseamnă actul de a trimite de date informatice altora, în timp ce prin "punere la dispoziţie" se înţelege plasarea online, pentru uzul altora. Acest concept intenţionează să acopere şi creaţia sau compilarea de legături către alte locaţii pe Internet (*hyperlink*-uri) pentru a facilita accesul la asemenea mecanisme/programe.

"Programele informatice" la care se referă textul de lege de la art. 365, în alin. 1 şi 2, sunt, spre exemplu, programele proiectate (realizate) să altereze sau chiar să distrugă date informatice sau să interfereze cu operaţiile sistemelor informatice, realizate sau adaptate pentru a controla/permite accesul în sisteme informatice (spre exemplu, cai troieni informatici sau alte tipuri de contaminanţi informatici).

A "deţine" astfel de dispozitive[764], programe informatice, parole, cod de acces sau a altor date informatice, în sensul variantei prevăzute la alin. 2, înseamnă

---

[764] Prin "dispozitiv" se înţelege ceva care face posibilă o ingerinţă de un anumit tip într-un sistem informatic; prin "program informatic" în acest context se înţelege un program capabil să distrugă date, să le altereze, să intercepteze date informatice sau să permită intrarea într-un sistem informatic; prin "parolă" se înţelege o secvenţă de caractere care serveşte la obţinerea accesului la un calculator sau sistem informatic; prin "cod de acces" se înţelege o secvenţă de caractere care permite autentificarea unui utilizator, permiţându-i acestuia accesul la un sistem

BOLYAI CENTRAL UNIVERSITY LIBRARY

a le avea în posesie (stocate, spre exemplu, în memoria calculatorului, pe discuri compact sau flexibile etc.).

Legiuitorul noului Cod penal, preluând formularea textului corespunzător de la nivel european a prevăzut în legătură cu toate activitățile prevăzute în alineatele textului art. 365, o singură cerința esențială: *fără drept*. Acest lucru semnifică un comportament neautorizat, care duce la afectarea unuia sau mai multor atribute ale securității sistemelor și datelor informatice: integritatea, confidențialitatea și disponibilitatea.

Urmarea imediată. Pentru întregirea laturii obiective, este necesar ca acțiunile incriminate să aibă ca urmare imediată crearea unei stări de pericol pentru integritatea, confidențialitatea sau disponibilitatea datelor sau sistemelor informatice prin creșterea posibilității de comitere a infracțiunilor prevăzute în art. 360-364 noul Cod penal.

Starea de pericol există în momentul în care acțiunile descrise în cele trei aliniate sunt realizate fără drept sau privesc dispozitive și programe informatice apte să realizeze cu succes infracțiunile de acces ilegal, intercepție neautorizată, alterarea ilegală a datelor informatice sau perturbarea funcționarii sistemelor informatice.

Latura obiectivă a infracțiunii de operațiuni ilegale cu dispozitive sau programe informatice nu este realizată decât atunci când starea de pericol pentru integritatea, confidențialitatea sau disponibilitatea datelor sau sistemelor informatice este urmarea imediată a acțiunilor de producere, punere în circulație (vânzare, import, distribuire, punere la dispoziție) sau deținere.

Legătura de cauzalitate. Este necesar ca între acțiunile incriminate și urmarea imediată să existe un raport de cauzalitate, care rezultă *ex re*.

B) Latura subiectivă

Elementul subiectiv. Pentru existența infracțiunii de operațiuni ilegale cu dispozitive sau programe informatice se cere ca fapta să fie săvârșită cu vinovăție. Forma de vinovăție necesară este *intenția (calificată prin scop)*.

Scopul. Pentru existența infracțiunii sub aspect subiectiv, în ambele variante normative, este necesară îndeplinirea unei condiții esențiale: acțiunile incriminate să fie realizate în *scopul săvârșirii uneia dintre infracțiunile prevăzute în art.* 360-364 noul Cod penal. În lipsa acestui scop, fapta nu va fi considerată infracțiunea prevăzută în art. 365 noul Cod penal.

Mobilul săvârșirii infracțiunii nu constituie element component al laturii subiective, însă stabilirea acestuia poate contribui – în fiecare caz concret – la o justă individualizare a pedepsei.

Forme, modalități, sancțiuni

A. Formele infracțiunii

a) **Actele pregătitoare** sunt posibile, dar ele sunt incriminate. Cum, în esență, faptele incriminate în textul de lege de față, sunt fapte

---

informatic sau la anumite servicii informatice. În *United States v. Patterson*, acuzatul a traficat pe un grup de știri Yahoo parole și alte informații, care permiteau altora acces la sistemul informatic al unei firme – vezi în *L.* Vasiu și L. Vasiu, *Dissecting Computer Fraud*, op. cit.

pregătitoare pentru infracţiunile prevăzute la art.360-364, este firesc ca legea să le incrimineze numai în forma consumată.

b) **Tentativa** este posibilă şi este incriminată (conform art. 366 noul Cod penal).

c) **Consumarea infracţiunii** are loc în momentul producerii urmării imediate (crearea stării de pericol prin comiterea uneia sau mai multor acţiuni incriminate).

d) **Epuizarea** are loc în momentul producerii ultimului act incriminat în textul de lege. Infracţiunea poate să se prezinte în forma continuă sau continuată. În cazul în cazul în care fapta este comisă în modalitatea deţinerii, infracţiunea are caracter continuu, epuizându-se la momentul încetării deţinerii ilicite.

B. Modalităţi

Modalitatăţi normative. O primă modalitate normativă este prevăzută în primul alineat al art. 365, lit. a) şi lit. b) care constă în fapta persoanei care, fără drept, produce, importă, distribuie sau pune la dispoziţie sub orice formă:

- dispozitive sau programe informatice concepute sau adaptate în scopul comiterii uneia dintre infracţiunile prevăzute în art. 360-364;
- parole, coduri de acces sau alte asemenea date informatice care permit accesul total sau parţial la un sistem informatic, în scopul săvârşirii uneia dintre infracţiunile prevăzute în art. 360-364.

Modalitatea normativă atenuată este prevăzută în cel de-al doilea alineat al art. 365 şi constă în deţinerea, fără drept, a unui dispozitiv, a unui program informatic, a unei parole, a unui cod de acces sau a altor date informatice dintre cele prevăzute în alin. (1), în scopul săvârşirii uneia dintre infracţiunile prevăzute în art. 360-364.

Modalitatăţile faptice se prezintă, datorită dezvoltării îngrijorătoare a pieţei de „instrumente a hackerilor", adică a *malware*, într-o diversitate de forme.

C. Sancţiuni

Pentru faptele prevazute în cele două variante normative ale art. 365, pedeapsa este închisoarea. Legiuitorul noului Cod penal reduce pedeapsa pentru cele două modalităţi faţă de pedeapsa din Legea nr. 161/2003. Pentru modalitatea prevăzută în primul alineat este închisoare de la 6 luni la 3 ani sau cu amendă, în cazul celei de-a doua, care este o variantă sancţionată mai puţin sever, pedeapsa este închisoarea de la 3 luni la 2 ani sau cu amendă.

Explicaţii complementare

A. Legătura cu alte infracţiuni: asemănări şi deosebiri

Cum evident reiese din textul de lege, infracţiunea de operaţiuni ilegale cu dispozitive sau programe informatice se află într-o strâsă legătură cu infracţiunile prevăzute la art. 360-364, fiind faţă de acestea, o „infracţiune mijloc".

BUCHAREST UNIVERSITY LIBRARY

Infracţiunea de operaţiuni ilegale cu dispozitive sau programe informatice, ca şi celelalte infracţiuni contra siguranţei şi integrităţii sistemelor informatice, este, cum am arătat deja, *subsidiară* faţă de alte infracţiuni datorită caracterului ei de generalitate (spre exemplu, infracţiunea incriminată de art. 32, lit.q) din Legea nr. 535/2004 privind prevenirea şi combaterea terorismului, articol modificat şi completat de art. 159 din Legea 187/2012 pentru punerea în aplicare a Legii nr.286/2009, *fraude comise prin sisteme informatice şi mijloace de plată electronice şi infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice).* Prin urmare, dacă se va realiza conţinutul infracţiunii de operaţiuni ilegale cu dispozitive sau programe informatice în condiţiile prevăzute de Legea nr. 535/2004 privind prevenirea şi combaterea terorismului (art. 32) vor fi incidente aceste prevederi, nu cele de faţă privitoare la infracţiunea de Operaţiuni ilegale cu dispozitive sau programe informatice.

B. Aspecte procesuale. Pentru infracţiunea prevăzută în acest text, acţiunea penală se pune în mişcare din oficiu, iar urmărirea penală este efectuată de către organele de cercetare penală, sub supravegherea procurorului.

C. Precedente legislative şi situaţii tranzitorii

a) Precedente legislative. Infracţiunea de operaţiuni ilegale cu dispozitive sau programe informatice este în totalitate preluată din art. 46 al Legii nr 161/2003, a cărei sursă este art.6 din Convenţia europeană privind criminalitatea informatică.

b) Situaţii tranzitorii. Limitele de pedeapsă fiind mai reduse în noul Cod penal, în cazul succesiunii de legi penale în timp se va face aplicarea dispoziţiilor din noul Cod penal.

Elemente de drept comparat

Cum sursa acestei incriminări este art. 6 din Convenţia europeană privind criminalitatea informatică, marea majoritate a statelor europene au prevederi similare în acest domeniu. Directiva din 2013 privind atacurile împotriva sistemelor informatice a fixat anul 2014 ca termen limită adaptarea legislaţiei naţionale în domeniu, pentru toate statele membre. Prezentăm câteva reglementări în domeniu ale unor ţări europene şi ne-europene, care, ca şi România, au infracţiunea de Operaţiuni ilegale cu dispozitive sau programe informatice în acord deplin cu art. 6 al Convenţiei europene în domeniul criminalităţii informatice.

Codul Penal Italian în art. 615-*quater* şi 615-*quinquies* prevede infracţiunea de operaţiuni ilegale cu dispozitive sau programe informatice *misuse of devices*). **Codul penal austriac**_prevede infracţiunea de operaţiuni ilegale cu dispozitive sau programe informatice *(misuse of devices)* în art. 126c.

Statele Unite ale Americii prevăd infracţiunea de operaţiuni ilegale cu dispozitive sau programe informatice *(misuse of devices)* în 18 USC § 1029 (*Fraud and related activity in connection with access devices*). Phishing-ul este adesea urmărit penal conform 18 USC § 1029[765] (uneori, cazurile din această categorie sunt aduse în instanţă şi sub 18 USC § 1028A. *Aggravated identity theft*). În **California**, *Anti-Phishing Act* din anul 2005 face ilegală, solicitarea de informaţii personale prin

---

[765] Vezi, spre exemplu, United States v. Boceanu, No. 07-CR-00012 (D. Conn. Feb. 4, 2013); United States v. Blount, No. 09-2139-cr (2d Cir. May 14, 2010).

BCU IASI / CENTRAL UNIVERSITY LIBRARY

intermediul unei pagini web sau a poştei electronice prin metoda prezentării ca o entitate legitima fără autorizarea sau aprobarea respectivei entităţi. **Sri Lanka** prevede infracţiunea de operaţiuni ilegale cu dispozitive sau programe informatice (*misuse of devices*) în Art. 9 din Computer Crime Act Nr. 24/2007 (FC).

4.7 Pornografia infantilă

Art. 374. (1) Producerea, deţinerea în vederea expunerii sau distribuirii, achiziţionarea, stocarea, expunerea, promovarea, distribuirea, precum şi punerea la dispoziţie în orice mod, de materiale pornografice cu minori, se pedepseşte cu închisoarea de la un an la 5 ani.
(2) Dacă faptele prevăzute în alin. (1) au fost săvârşite printr-un sistem informatic sau alt mijloc de stocare a datelor informatice, pedeapsa este închisoarea de la 2 la 7 ani.
(3) Accesarea, fără drept, de materiale pornografice cu minori, prin intermediul sistemelor informatice sau altor mijloace de comunicaţii electronice, se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă.
(4) Prin materiale pornografice cu minori se înţelege orice material care prezintă un minor având un comportament sexual explicit sau care, deşi nu prezintă o persoană reală, simulează, în mod credibil, un minor având un astfel de comportament.
(5) Tentativa se pedepseşte.

Introducere

Natura deschisă şi sofisticată a societăţii informaţiilor şi comunicaţiilor, oferă oportunităţi fără precedent pentru realizarea şi distribuirea materialelor cu conţinut pornografic şi obscen. Conform unor cifre din anul 2005, numărul estimat de pagini web pornografice era de peste 260 milioane, 28 milioane pagini noi fiind adăugate în fiecare lună, sumele cheltuite pentru pornografie pe Internet erau estimate la 57 miliarde global (12 miliarde în SUA)[766]. Ca mediu de comunicare în masă, Internetul este utilizat extensiv în legătură cu materialele de natură sexuală, în special pentru vânzarea şi procurarea de materiale pornografice, de echipamente erotice, pentru publicitatea contactelor pentru scopuri explicit sexuale şi pentru distribuirea materialelor cu conţinut de exploatare a copiilor, furnizând şi o platformă pentru grooming-ul online al copiilor[767].

Exploatarea sexuală a copiilor este o formă gravă de violenţă împotriva acestora. Conform UNICEF, circa două milioane de copii sunt folosiţi în industria sexului în fiecare an, iar pe Internet există peste un milion de imagini ale copiilor abuzaţi[768]. Principalul instrument internaţional în domeniul protecţiei drepturilor copiilor, inclusiv împotriva exploatării sexuale, este Convenţia Naţiunilor Unite

766 Vezi J. Chrislip, *Filtering the Internet Like a Smokestack: How the Children's Internet Protection Act Suggests a New Internet Regulation Analogy*, Journal Of High Technology Law, Vol. V No. 2, 2005.

767 Vezi United Nations, *Draft resolution I, op.cit.*

768 Vezi Council of Europe, *Raportul explicativ* al *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (CETS No. 201).

BCU IASI / CENTRAL UNIVERSITY LIBRARY

din anul 1989. Convenția protejează copiii împotriva tuturor formelor de exploatare și abuz sexual, Națiunile Unite considerând că protecția acordată în cyberspațiu copiilor trebuie să fie similară celei din lumea fizică[769].

Camerele digitale, anonimitatea și posibilitatea de a încărca rapid fotografii pe Internet oferă celor care săvârșesc pornografia infantilă și alte abuzuri asupra minorilor[770] căi extrem de eficiente pentru îndeplinirea scopurilor, în unele cazuri fără ca victimele să manifeste suspiciuni. Cei care săvârșesc astfel de fapte utilizează adesea rețele de socializare pentru a localiza și contacta viitoarele victime, dar și pentru a comunica cu alți pedofili, printre făptuitori numărându-se bărbați și femei[771]. Fetele sunt considerate a fi mai expuse riscului de victimizare de crime sexuale inițiate pe Internet.

Unii autori consideră că obsesia umană în ceea ce privește pornografia și obscenitatea este la fel de veche ca societatea insăși[772], dar tehnologiile avansate, mai ales Internetul mobil, au făcut deosebit de atractiv mediul digital pentru abuzuri împotriva minorilor și deosebit de complicat răspunsul la întrebarea-cheie: Cum poate dreptul să reglementeze aceste noi provocări?[773]. Primul acord de angajament internațional important în domeniul eliminării distribuirii de materiale care privesc exploatarea sexuală a copiilor pe Internet a înregistrat la Conferința Internațională "Combating Child Pornography on the Internet" (Viena, 1999), unde s-a statuat că *pornografia cu copii pe Internet este o problemă în continuă creștere și pe măsură ce lumea online devine din ce în ce mai vastă, va continua să crească în viitor, de vreme ce granițele statelor nu mai prezintă o opreliște.*

Evaluarea precisă a magnitudinii fenomenului de criminalitate împotriva copiilor online este foarte dificil de realizat[774]. O estimare a Virtual Global Taskforce sugerează că există peste 100000 de site-uri web care afișează imagini cu copii abuzați, iar 1 din 5 copii care utilizează Internetul au primit solicitări nedorite pentru activități sexuale[775]. Internet Crimes Against Children (ICAC) raportează un număr de 5300 arestări pentru infracțiuni privind pornografia infantilă în anul fiscal 2010, o creștere de 150% față de anul 2006 (pedepsele

---

769 United Nations, Commission on Crime Prevention and Criminal Justice, *Draft resolution I - Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children*, 2011.

770 Vezi o discuție a riscurilor la adresa minorilor în F. Casarosa, *Protection of Minors Online: Available Regulatory Approaches*, Journal of Internet Law, March, 2011.

771 Vezi cazuri din Regatul Unit, menționate în E. Martellozzo, D. Nehring și H. Taylor, *Online child sexual abuse by female offenders: An Exploratory study*, International Journal of Cyber Criminology, Jan – July, July - December (*Combined Issue*), Vol. 4 (1&2), 592–609, 2010.

772 Vezi un istoric al pornografiei și obscenității în A. Murray, *Information Technology Law. The law and society*, Oxford University Press, 2010, p. 353.

773 Întrebări de acest gen au fost puse încă de la începuturile utilizării Internetului, unii autori propunând măsuri radicale, de tipul cenzurii; a se vedea, în acest sens, P. Johnson, *Pornography drives Technology: Why not censor the Internet?*, Federal Communications Law Journal 217, 1996.

774 Vezi C. Bialik, *Measuring the child-porn trade*, Wall Street Journal, 18 April 2006.

775 Vezi http://www.virtualglobaltaskforce.com/report-abuse; http://www.virtualglobaltaskforce.com/2011/international-experts-meet-to-collaborate-against-child-sexual-predators/.

BCU IAȘI / CENTRAL UNIVERSITY LIBRARY

pentru astfel de infracţiuni sunt aspre, putând fi închisoare până la 10 ani)[776], iar Internet Crime Complaint Center a referit 2597 plângeri privind pornografia infantilă către National Center for Missing and Exploited Children[777].

Cybercriminalii în domeniu pot să își găsească victimele utilizând diverse tehnici sau medii digitale[778], cum ar fi:

• Conturile de mesagerie instant (MSN messenger etc.), unde, de regulă, detalii despre utilizator, inclusiv cele legate de vârstă, pot fi vizualizate public dacă deţinătorul contului nu stabileşte altfel;

• Site-urilor web pentru jocuri, care, pe lângă serviciile specifice (furnizare a jocurilor) permit comunicarea între jucători la nivel global;

• Chat şi forumurile de discuţii, unde cybercriminalii pot atrage copii, ademenindu-i prin adulări sau inducându-i în eroare pentru a comunica într-un mod mai privat (prin SMS sau prin serviciile de mesaje instant);

• Poşta electronică, făptuitorii trimiţând adesea mesaje frauduloase, în care pretind că reprezintă o asociaţie care este interesantă pentru copil, în speranţa că vor stabili o comunicare privată cu minorul.

Expunerea la abuzuri a minorilor în societatea digitală este foarte mare: materialele pornografice sunt găzduite pe mii de servere aflate în lumea întreagă. Făptuitorii au simţit potenţialul imens şi utilizează gratuit şi la adăpostul anonimității sistemele de *file-sharing* sau folosesc Internetul mobil pentru a transmite materiale cu conţinut pornografic. Fiind o societate globală şi expunerea la asemenea riscuri este globală. Ideal ar fi un standard global care să fie luat în considerare la stabilirea caracterului pornografic al materialelor care sunt expuse ori transmise în acest mediu digital.

Într-un studiu amplu despre riscurile şi securitatea minorilor online, realizat la nivelul Uniunii Europene[779], se arată că peste 23% dintre minorii cu vârsta între 9 şi 16 ani au văzut materiale pornografice (cu conţinut explicit sexual) pe Internet în ultimele 12 luni. Consiliul Europei şi Parlamentul European au ajuns la un acord

---

776 Vezi US Government Accountability Office (GAO), *Combating child pornography*, 2011; vezi şi C. Marcum, G. E. Higgins, T. L. Freiburger şi M. L. Ricketts, *Policing possession of child pornography online: investigating the training and resources dedicated to the investigation of cyber crime*, International Journal of Police Science & Management, 12, 516–525, 2010.

777 Vezi Internet Crime Complaint Center, *2010 Internet Crime Report*, 2011.

778 Vezi UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, 2014.

779 Titlul studiului este *EU Kids Online II: Enhancing Knowledge Regarding European Children's Use, Risk and Safety Online*; proiectul a fost finanţat de EC Safer Internet Programme (contract SIP-KEP-321803). Scopul său principal este creşterea gradului de cunoaştere în ceea ce priveşte experienţa şi practicile copiilor şi părinţilor lor privitor la risc şi siguranţă pe Internet şi în cadrul altor tipuri de tehnologii, pentru a determina actorii principali la nivel internaţional să adopte măsurile necesare pentru creşterea siguranţei copiilor online. Adoptând o abordare centrată pe copil, comparativă, critică şi contextuală, studiul EU Kids Online a construit şi condus un sondaj despre experienţa riscului online în rândul copiilor între 9 şi 16 ani din 25 de ţări europene (inclusiv România); rezultatele au fost şi vor fi prezentate în cadrul mai multor conferinţe şi întâlniri de impact în perioada 2010-2012; pentru mai multe informaţii, vezi www.eukidsonline.net.

politic şi au propus Directiva 2011/93/UE Parlamentului European şi a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor şi a pornografiei infantile şi de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului. Conform acestei Directive, "pornografia infantilă, care constă în imagini cu copii supuşi unor abuzuri sexuale, reprezintă un tip specific de conţinut care nu poate fi considerat ca exprimare a unei opinii".

Directiva 2011/93/UE defineşte conceptul de "pornografie infantilă" ca fiind:

(i) orice material care prezintă vizual un copil care este implicat într-un comportament sexual explicit, real sau simulat;

(ii) orice reprezentare a organelor genitale ale unui copil în principal cu scop sexual;

(iii) orice material care prezintă vizual orice persoană care pare a fi un copil implicat într-un comportament sexual explicit, real sau simulat, sau orice prezentare a organelor sexuale ale unei persoane care pare a fi un copil, în principal cu scop sexual; sau

(iv) imagini realiste ale unui copil implicat într-un comportament sexual explicit sau imagini realiste ale organelor sexuale ale unui copil, în principal cu scop sexual.

Directiva ţinteşte armonizarea a aproximativ 20 de infracţiuni cu relevanţă în domeniul exploatării sexuale a copiilor şi a pornografiei infantile, grupate astfel: în Art. 3 - *Infracţiuni referitoare la abuzul sexual*; în Art. 4 - *Infracţiuni referitoare la exploatarea sexuală*; în Art. 5 - *Infracţiuni referitoare la pornografia infantilă*; iar în Art. 6 - *Ademenirea copiilor în scopuri sexuale*. Un număr de prevederi sunt consacrate investigaţiei şi iniţierii procedurilor de către organele abilitate, infracţiunilor comise în străinătate, protecţiei victimei şi prevenirii comiterii de infracţiuni în domeniu.

Cu privire la pornografia infantilă, Directiva obligă statele membre să închidă prompt site-urilor web care găzduiesc pornografie. Adiţional, statele membre pot bloca accesul la astfel de pagini web, dar trebuie să o facă respectând procedurile de transparenţă. De asemenea, Directiva loveşte puternic în aşa-numita industrie de turism sexual, în special prin măsuri preventive, care să micşoreze cererea de servicii sexuale din afara UE. Mai mult, o prevedere importantă se referă la obligaţia statelor de a nu permite celor care au fost pedepsiţi pentru infracţiuni în domeniu să desfăşoare activităţi profesionale care implică contactul regulat cu copiii.

Cadrul legal actual în domeniul pornografiei infantile, în aşteptarea completărilor şi modificărilor prevăzute de această Directivă, dar şi a Tratatului global în domeniul cybercriminalităţii şi cybersecurităţii[780], conţine mai multe reglementări juridice internaţionale: Convenţia Naţiunilor Unite privind drepturile copilului (*Convention on the Rights of the Child*); Protocolul facultativ la Convenţia privind drepturile copilului, referitor la vânzarea de copii, prostituţia

[780] Vezi S. Schjolberg şi S. Ghernaouti-Helie, *A Global Treaty on Cybersecurity and Cybercrime*, Second edition, 2011.

copiilor și pornografia infantilă (*Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography*); Rezoluția Națiunilor Unite 2011/33 (*Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children*); Convenția Consiliului Europei privind criminalitatea informatică; Convenția Consiliului Europei privind protecția copiilor împotriva exploatării sexuale și a abuzului sexual; Convenția privind interzicerea și luarea imediată de atitudine în scopul eliminării celor mai grave forme de exploatare prin muncă a copilului[781].

Posesia de pornografie cu copii online este ilegală în multe state; cu toate acestea, mai sunt multe state (în particular cele din Sud-Estul Asiei) care nu au legi corespunzătoare în domeniu pentru a face față fenomenului, pornografia infantilă în sistemele informatice fiind acolo o industrie înfloritoare[782].

România, țară semnatară și ratificantă a Conventiei Europene privind criminalitatea informatică, a încercat să creeze un cadru legal adecvat, care să facă față acestui fenomen grav. Cadrul legal, până la intrarea în vigoare a noului Cod penal, era cuprins, în principal, în trei acte normative care conțin incriminări în domeniul pornografiei infantile: pornografia infantilă în varianta tip prevăzută de Legea nr. 678/2001 privind prevenirea și combaterea traficului de persoane și de Legea nr. 196/2003 privind prevenirea și combaterea pornografiei; pornografia infantilă prin sisteme informatice, care reprezinta infracțiunea specială și era prevăzută de Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției.

Operațiunile întreprinse în multe țări la nivel global au identificat mii de făptuitori în domeniul infracțiunilor de abuz asupra copiilor, numărul acestora fiind în creștere în ultimii ani, ceea ce confirmă creșterea prognozată la Conferința de la Viena din anul 1999. Lupta împotriva exploatării sexuale a copiilor, inclusiv proliferarea materialelor pornografice cu copii pe Internet, este o provocare continuă pentru organele de investigație și cele de judecată, datorită inovațiilor tehnologice. Succesul unei strategii de luptă în domeniu nu mai poate urma o singură cale (cea traditională) de construire a unui cadru legal. Pe lângă o strategie normativă, cât se poate de armonizată și adaptată realității, o strategie efectivă a unui parteneriat complex este strict necesară. Acest parteneriat ar trebui să cuprindă agenții de implementare a legislației, autorități judiciare, reprezentanți din industria tehnologiilor informației și comunicațiilor, furnizori de servicii Internet, reprezentanți ai sectorului bancar[783] și organizațiile nonguvernamentale.

---

781 Vezi și A. S. Reid, *Online protection of the child within Europe*, International Review of Law, Computers & Technology, Vol. 23, No. 3, 217-230, 2009.

782 Vezi http://www.unicri.it/emerging_crimes/cybercrime/explanations/children.php.

783 Încă din anul 2006, International Centre for Missing and Exploited Children (ICMEC), o organizație nonguvernamentală cu sediul în SUA, împreună cu organizația-soră National Center for Missing and Exploited Children (NCMEC) a lansat Coaliția Financiară Împotriva Pornografiei cu copii (Financial Coalition Against Child Pornography), iar în septembrie 2011 aceasta a fost întărită, încercându-se tăierea fluxului de bani care susține acest tip de pornografie. A se vedea, în acest sens, *Disrupting the flow of funds that support the child*

În cele mai multe state membre ale UE, nevoia de a stabili o colaborare strânsă între organele de punere în aplicare a legii şi furnizorii de servicii Internet a fost deja identificată, atât la nivel de prevenire, cât şi în etapa investigaţiei[784]. Furnizorii de servicii Internet pot să asigure asistenţă prin furnizarea de date care pot fi utilizate în identificarea, cercetarea şi pedepsirea făptuitorilor; de asemenea, pot să ajute prin adoptarea de proceduri şi coduri de comportament care pot limita exploatarea copiilor de către făptuitori pe Internet. Un pas pozitiv este şi faptul că multe state membre au înfiinţat departamente specializate pentru combaterea pornografiei pe Internet.

Pentru a realiza o strategie complexă şi completă, trebuie să se ţină seama de tendinţele activităţii criminale în acest domeniu[785], realităţi periculoase care cer o atenţie deosebită. Principalele direcţii de dezvoltare se bazează pe următoarele tendinţe criminale:

• Criminalii se focalizează pe canale ascunse (reţele *peer-to-peer*[786], oferirea de site-uri web cu pornografie pe sistemul *pay-per-view* este într-o anumită descreştere, datorită acţiunii organelor de ordine la nivel internaţional), unde accesul este acordat numai unor utilizatori "selectaţi" (selecţia este realizată de cel care deţine canalul respectiv, bazată pe calitatea/cantitatea imaginilor pornografice care pot fi schimbate şi chiar pe nivelul de încredere şi respect reciproc);

• Criminalii de acest gen şi reţelele lor utilizează, din ce în ce mai mult, programe informatice sofisticate pentru a reduce evidenţele digitale permanente[787], a-şi proteja anonimitatea, pentru a face uz de stocările online şi utilizează tehnici avansate de criptare pentru a contracara expertizele criminalistice dispuse de poliţie în mediul digital;

• Criminalii călătoresc în anumite ţări unde copiii sunt oferiţi de familiile lor, sau alte persoane joacă rolul de intermediari în scopul de a exploata sexual sau a produce materiale pornografice cu minori, materiale care să fie apoi distribuite pe Internet;

• Materialele pornografice sunt, uneori, produse chiar de adolescenţi sau copii care subestimează riscurile la care se expun prin transmiterea sau stocarea unor astfel de imagini sau materialelor video[788];

---

pornography business, http://www.virtualglobaltaskforce.com/2011/disrupting-the-flow-of-funds-that-support-the-child-pornography-business/.

784 Vezi EUROPOL, *Child Sexual Exploitation Fact Sheet 2011*, p. 4.

785 Vezi United Nations Congress on Crime Prevention and Criminal Justice, *Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime*, Working paper prepared by the Secretariat, 2010.

786 Vezi US GAO, *File Sharing Programs: The Use of Peer-to-Peer Networks to Access Pornography*, 2005.

787 Spre exemplu, folosind aplicaţii precum "SnapChat" sau "Wickr", vezi S. Henn, *Teens Dig Digital Privacy if SnapChat is any Indication*, 2013.

788 Vezi ce a pregătit FBI pentru părinţi în încercarea de a le oferi un ghid pentru educarea copiilor, *Parent's Guide to Internet Safety*.

BCU CLUJ / CENTRAL UNIVERSITY LIBRARY

• În unele cazuri, copiii sunt forțați sau îndemnați la producerea materialelor pornografice de către acest tip de făptuitori, prin *grooming*;

• Creșterea cazurilor de *groming* online și solicitarea de mesaje sexuale prin intermediul telefoanelor mobile și al echipamentelor multimedia (fenomenul de "sexting"[789]).

Problema cea mai stringentă și importantă, după incriminarea pornografiei infantile prin sistemele informatice în coduri penale naționale sau în legi speciale[790], este modul în care este calificată de către legiuitor această formă de activitate criminală, modul în care este implementat textul de lege în activitatea organelor judiciare și mai ales politicile de prevenire care ar trebui să existe în acest domeniu. Practica judiciară a multor state a relevat, de-a lungul timpului (ne referim aici și la pornografia în mediul clasic, nu numai în cel digital), faptul că implementarea a fost dificilă, în special datorită nedefinirii sau definirii necorespunzătoare a termenilor-cheie utilizați de legiuitor. Mai mult, multiplele fațete prezentate de tehnologiile de ultimă oră pun la grea încercare legiuitorul și practicianul zilelor noastre.

De altfel, nici Convenția Europeană privind criminalitatea informatică, care a urmărit să răspundă acestor provocări propunând un standard global în domeniu[791], nu definește toți termenii-cheie utilizați în art. 9 (articol consacrat pornografiei infantile în sistemele informatice), ci revine, în Raportul Explicativ, cu explicații suplimentare[792]. Din păcate, nu toate statele au prevăzut definiții precise ale unor termeni esențiali cu care lucrează legiuitorul, cum sunt: "pornografic", "indecent", "obscen", "erotic" și, din acest motiv, aplicarea diferită în practică este des întalnită, determinarea caracterului indecent sau obscen al unui material rămânând, de regulă, la aprecirea judecătorului[793]. Foarte sugestiv este exemplul pe care, cu ironie amară, îl dă celebrul profesor de la Universitatea Harvard, Alan Dershowitz, în cartea sa "The best defence", în legătură cu lipsa unei definiții unanim acceptate a pornografiei, cel al unui judecător al Curții Supreme a SUA, care a spus "nu știu să definesc pornografia, dar o recunosc când o văd"[794].

---

[789] Vezi D. T. Sacco și colab., *Sexting: Youth Practices and Legal Implications*, Berkman Center for Internet & Society, Harvard University, 2010.

[790] Vezi art. 51 din Legea nr. 161/2003, care reproduce art. 9 din Convenția europeană privind criminalitatea informatică.

[791] Convenția a fost semnată și ratificată nu numai de state din Europa, ci și de alte state, cum ar fi SUA, care a și participat la lucrările de elaborare a acesteia.

[792] Definiția pe care o dă în Raportul explicativ legiuitorul european conceptului-cheie de "comportament sexual explicit" este cea utilizată de legiuitorul american în Titlului 18 din U.S. C., Partea I, Capitolul 110, Sectiunea 2256, alin. 2.

[793] Vezi, pentru SUA, cazul *Miller v. California*, 413 U.S. 15 (1973); acesta a fost un caz important al Curții Supreme a SUA și a implicat materiale cu caracter obscen care nu sunt ocrotite prin prevederile constituționale referitoare la libertatea de expresie. Decizia din acest caz stabilește ceea ce a fost ulterior numit "Miller test", care definește „material cu caracter obscen"; a se vedea, pentru amănunte, J. Tuman, *Miller v. California*, 2003, în R. A. Parker (ed.). *Free Speech on Trial: Communication Perspectives on Landmark Supreme Court Decisions*. Tuscaloosa, AL: University of Alabama Press, p. 187–202.

[794] Vezi A. Dershowitz, *The best defence*, New York, Random House, 1982. Vezi și discuția

BCU IASI / CENTRAL UNIVERSITY LIBRARY

Stabilirea liniei de demarcaţie între materialul cu conţinut indecent şi cel obscen este una foarte importantă pentru aplicarea corectă a textelor de lege în domeniu. Materialul pornografic poate fi indecent sau obscen, doar materialul obscen este cel care nu poate fi publicat, distribuit sau importat. Cu alte cuvinte, o persoană poate să comercializeze în mod legal un material cu conţinut considerat indecent, atât timp cât este în conformitate cu legislaţia în vigoare, dar nu poate comercializa material cu conţinut obscen.

Aşadar, în momentul în care eroticul a făcut loc pornografiei şi obscenităţii, dreptul a început să se implice în controlul produselor pornografice; intervenţia principală fiind trasarea liniei de demarcaţie între tipurile de erotografie: *material cu conţinut erotic* (cum ar fi diversele forme de artă: pictură, sculptură, fotografie sau literatură erotică)[795]; *material cu conţinut obscen*[796] şi *material cu conţinut pornografic extrem* (acesta cuprinde imagini cu copii abuzaţi şi conţinut violent sau obscen extrem). Imaginile care reprezintă pornografia cu caracter extrem (imagini care prezintă asfixie sexuală, necrofilie, viol etc.) sunt considerate de toate legislaţiile actuale ca aducând un abuz grav la adresa minorilor[797]. Într-un astfel de caz[798], cinci persoane, membri ai grupului Quest4More, au primit pedepse între 7 şi 15 ani pentru susţinerea torturii sexuale a copiilor.

Materialele cu conţinut erotic sunt, de regulă, distribuite şi vândute în mod liber şi, în mod normal, cu foarte puţine restricţii. În mediul clasic, spre exemplu, unele librării au o secţiune de literatură erotică, aceasta neînsemnând neapărat că nu vor vinde unui minor cărţi care se înscriu în această zonă (spre exemplu, Fanny Hill sau Tropic of Cancer), deşi unii vânzători refuză să o facă (poziţie personală, nu una cerută de lege). În ceea ce priveşte mediul online, în mod particular cel al reţelelor de socializare, este foarte dificil să se restricţioneze accesul minorilor la materialele pentru adulţi.

În SUA, legiuitorul a încercat să reglementeze domeniul încă de la începuturile utilizării în masă a Internetului. Astfel, în anul 1996, două încercări au stârnit controverse majore: guvernatorul statului New York a introdus în Codul penal al statului un text care face infracţiune diseminarea de informaţii periculoase pentru minori prin intermediul sistemelor informatice, iar Guvernul federal a introdus *Communications Decency Act* (1996) ca Titlul V al Telecommunications Act 1996. Ambele măsuri au fost considerate ca aducând atingeri Constituţiei SUA

---

cazului New York v. Ferber şi decizii ale Curţii Supreme în D. T. Sacco şi colab., *Sexting: Youth Practices and Legal Implications*, Harvard University, 2010 şi definiţia din Protocolul facultativ la Convenţia privind drepturile copilului, referitor la vânzarea de copii, prostituţia copiilor şi pornografia infantilă.

795 Acest tip de material este definit in Regatul Unit în secţiunea 63(3) a Criminal Justice and Imigration Act 2008 ca fiind materialul produs în jurul unei teme sexuale, dar nu este produs în totalitate sau în principal în scopul excitării sexuale (*sexual arousal*).

796 În conformitate cu definiţia dată de s1(1) din Obscene Publication Act 1959 din Regatul Unit, acest material se consideră că poate să ducă la depravarea şi coruperea persoanelor.

797 Vezi, în acest context, şi A. D. Murray, *The Reclassification of Extreme Pornographic Images*, The Modern Law Review, 72(1), 73-90, 2009.

798 Vezi US DoJ, Release No. 11-093, June 27, 2011.

(a se vedea First Amendament[799]) şi au fost atacate în justiţie de mai multe grupuri sau asociaţii (printre care cele mai importante: American Library Associations, Peacefire şi American Civil Liberties Associations). În acest caz, este deosebit de relevantă decizia judecătoarei Loretta Preska, care a fost în favoarea celor care au formulat plângerea, subliniind în motivare că sunt prea generale conceptele folosite de legiuitor şi, prin urmare, ar putea duce chiar la interzicerea unor opere literare şi artistice[800] (mulţi artişti îşi postează operele pe Internet, aşa că ar putea fi consideraţi infractori, în conformitate cu asemenea prevederi legislative[801]).

În anul 2008, Preşedintele Bush a semnat *Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act*. Conform acestui Act, Departmentul Justiţiei formulează şi implementează Strategia naţională pentru combaterea exploatării copiilor. Combaterea acestui fenomen infracţional implică numeroase entităţi: FBI, care, în anul 2010, spre exemplu, a investigat 6070 cazuri şi a arestat 1094 persoane; The Innocent Images National Initiative, o componentă a a Cyber Division a FBI; The Child Exploitation and Obscenity Section (CEOS), o unitate a Criminal Division din cadrul Departamentului Justiţiei (DoJ), specializată în infracţiunile de exploatare sexuală a minorilor la nivel federal; 94 Attorneys' Offices; Internet Crimes Against Children, program creat de DoJ în anul 1998, administrat şi finanţat prin Office of Juvenile Justice and Delinquency Prevention (OJJDP), care, în anul 2010, a investigat 32300 cazuri şi a arestat 5300 persoane; Secret Service, care, în anul 2010, a investigat 188 cazuri şi a făcut 149 arestări; Immigration and Customs Enforcement (ICE), care a investigat 2622 cazuri şi a făcut 931 arestări în anul 2010; Postal Service[802]. Un număr de organizaţii nonguvernmentale lucrează cu agenţiile federale, statale, locale şi partenerii tribali pentru combaterea acestui fenomen: National Center for Missing & Exploited Children, Child Help, Darkness to Light, Girls Educational and Mentoring Services, Inc., Enough is Enough, i-Safe, Kristi House, Inc., Nevada Child Seekers, Paul and Lisa Program, Inc., Web Wise Kids, San Diego Police Foundation, Self-Reliance Foundation, Washtenaw Area Council for Children, INOBTR, TechMissionYouth Program, PROTECT, ECPAT-USA etc.[803]

Cazurile studiate dau o imagine mai clară a fenomenului. Astfel, într-un caz din anul 2009, făptuitorul a încercat să realizeze profit din pozele nud ale unei adolescente, obţinute în urma preluării controlului asupra contului de poştă electronică şi a conturilor ei de pe reţelele de socializare (investigaţia FBI a condus la o sentinţă de 18 ani pentru infractorul în cauză, arătându-se că astfel de fapte nu vor fi tolerate[804]). În anul 2009, *Operation Delego*, desfăşurată sub egida

---

799 Vezi M. P. Goldstein, *Congress and the Courts Battle over the First Amendment: Can the Law Really Protect Children from Pornography on the Internet?*, 21 J. Marshall J. Computer & Info. L. 141, 2003.

800 În motivarea deciziei, au fost date exemple de opere de artă faimoase, cum ar fi cele ale lui Botticelli, Manet, Matisse etc., care pot fi găsiţi pe Internet.

801 Vezi decizia din cazul American Libraries Association v. Pataki, 20 iunie 1997.

802 Vezi detalii în US GAO, op. cit.

803 Vezi *The national strategy for child exploitation prevention and interdiction*, A Report to Congress, 2010.

804 Vezi G. M. Snow, *Statement before the House Judiciary Subcommittee on Crime, Terrorism,*

Department of Homeland Security, cu cooperare internațională (Eurojust și alte agenții naționale), a vizat rețeaua de pedofili Dreamboard, care avea circa 600 de membri și care se estimează că a distribuit circa 123 teraocteți de pornografie infantilă (echivalentul a circa 16.000 DVD-uri), a rezultat în mai multe arestări în 13 țări[805].

Pentru a nu mai exista atâtea diferențe de opinie și decizii controversate, s-a propus, inclusiv de Internet Watch Foundation, să nu mai fie utilizați termeni de genul "pornografie cu copii", "pornografie infantilă", propunându-se expresia-cheie "imagini care abuzează minori"[806], astfel de imagini fiind considerate a face parte din categoria materialelor cu conținut pornografic extrem și, după orice standarde, acestea sunt considerate materiale de natură obscenă, toate țările fiind în acord perfect că acestea trebuie considerate materiale ilegale. Un alt aspect important în legătură cu materialele pornografice în mediul digital este cel privind vârsta copilului din imagini, vârsta consimțământului copilului diferind de la o țară la alta: în Canada este 14 ani, în Regatul Unit este 16 ani, în USA diferă în funcție de stat, de la 16 la 18 ani, în Tunisia este 20 de ani, iar în Tonga este 12 ani[807]. Convenția europeană în domeniul criminalității informatice prevede vârsta de 18 ani (o țară semnatară a Convenției poate să stabilească și o limită de până de 16 ani, dar nu mai mică)[808].

Unele țări cer ca producătorii de filme pornografice să țină evidențe foarte clare în legătură cu vârsta actorilor[809]. În SUA, obligația este prevăzută de Child Protection and Obscenity Act; în Regatul Unit, nu este necesară o asemenea evidență strictă, dar nu este chiar atât de îngăduitoare ca în Suedia, care definește un copil ca fiind o persoană a cărui pubertate nu este încă încheiată, lucru observabil din imagine sau din alte circumstanțe, și care are mai puțin de 18 ani.

Tehnologii digitale de ultimă oră fac posibilă realizarea materialelor pornografice cu minori fără imaginea reală a unui copil (așa-numitele *pseudoimagini*). Imaginile generate de calculator nu trebuie confundate cu imagini în care imaginea unei persoane reale este manipulată sau schimbată (*morphed images*) sau cu imagini de tip "cut and paste", în care imaginea unei persoane reale este suprapusă pe imaginea altei persoane reale (spre exemplu, punerea capului unei persoane pe corpul alteia[810]). Intenția legiuitorului european de a incrimina și

---

and Homeland Security Washington, D.C. July 28, 2010. Vezi și http://www.fbi.gov/stats-services/publications/innocent-images-1/innocent-images-national-initiative.

805 Vezi *Secretary Napolitano and Attorney General Holder Announce Largest U.S. Prosecution of International Criminal Network Organized to Sexually Exploit Children*, Release Date: August 3, 2011.

806 Un raport al acestei fundații din anul 2010, arată că URL-urile care găzduiesc conținut care aduce atingere minorilor a crescut semnificativ în anul 2010 față de anul 2009: 48.702 raportări, o creștere de 27.9% față de anul 2009.

807 Vezi un tabel cu vârsta consimțământului din punctul de vedere al legilor naționale în S. Ghernaouti-Hélie, *Information Security for Economic and Social Development*, United Nations, ST/ESCAP/2505, 2008.

808 Vezi art. 9 (3) din Convenția Europeană privind criminalitatea informatică.

809 Vezi această obligație în US Child Protection and Obscenity Act (1998).

810 Vezi S. S. Kreston, *Defeating the Virtual Defense in Child Pornography Prosecutions*, 4 Journal of High Technology Law 49, 2004.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

aceste pseudoimagini reiese cu claritate din definiţia dată *materialelor pornografice cu minori*[811], definiţie preluată şi de legiuitorul român.

Crearea pseudo-imaginilor implică programe informatice (spre exemplu, cele realizate de Adobe sau Corel), fie pentru a crea imagini fotorealistice care arată copii abuzaţi sexual sau care manipulează imagini fotografice preexistente pentru a-i face pe actorii adulţi să arate ca nişte copii prin înlăturarea digitală a unor elemente (păr pubian sau din alte părţi ale corpului sau micşorarea organelor genitale sau a sânilor). În Regatul Unit, spre exemplu, pseudoimaginile sunt considerate un tip nou de imagini care constituie abuz asupra minorilor. Acest tip de imagini ridică în Regatul Unit o serie de probleme: ar trebui să fie interzise şi sancţionate de legea penală?

Spre deosebire de imaginile reale ale copiilor, pseudoimaginile sunt diferite. O analogie este făcută cu aceea a actorilor care joacă diferite roluri: în acelaşi fel în care actorii nu sunt cu adevărat loviţi sau omorâţi în filmele de acţiune violente sau în cele horror, nici copiii nu sunt afectaţi de aceste pseudoimagini. Aceste imagini pot fi văzute ca nişte extensii ale altor forme "artistice", care prezintă violenţa sau abuzul împotriva copiilor, cum ar fi personajele japoneze Manga sau Hentai. Cu toate acestea, sunt argumente cu caracter general care fac ca aceste pseudoimagini să nu poată fi trecute uşor cu vederea: există evidenţe care arată o strânsă legatură între imagini cu copii abuzaţi şi actul de abuz în sine[812].

Cu toate aceste discuţii şi controverse, Regatul Unit a fost printre primele state care a incriminat pseudoimaginile în Criminal Justice and Public Order Act 1994, extinzând atât incriminarea din Criminal Justice Act 1988, cât şi din Children Protection Act 1978, pentru a acoperi aceste imagini (a se vedea sectiunea 84 din Criminal Justice and Public Order Act care a făcut ajustările necesare la secţiunea 160 a Criminal Justice Act 1988)[813]. "Pseudofotografia" este definită de secţiunea 7(7) a Children Protection Act ca fiind "o imagine, fie realizată prin grafică de calculator, fie într-un alt mod, care pare o fotografie"[814]. Incriminarea acestor pseudoimagini la nivel internaţional este una esenţială în era digitală, lucru subliniat şi de legiuitorul european în Raportul Explicativ al Convenţiei: societatea informaţiei este o societate globală, existenţa unor ţări care nu aplică aceste standarde internaţionale face imposibilă îndeplinirea obiectivelor asumate de a proteja copiii împotriva abuzurilor[815].

---

811 Vezi art. 9 (2 (b,c)) din Convenţia Europeană privind criminalitatea informatică, text preluat şi de Legea nr. 161/2003, în art. 5, lit. i; acest text este reprodus şi de noul Cod penal (varianta 2011), în art. 372.

812 Vezi un studiu realizat în anul 2003 J. Wolak, R. Mitchell şi D. Finkelhor, *Internet Sex Crimes Against Minors:The Response of Law Enforcement*, Crimes against Children Research Center, University of New Hampshire, 2003.

813 Vezi secţiunea extinsă s 1(1) din Children Protection Act şi sectiunea 160(1) din Criminal Justice Act, care statuează că este infracţiune posesia de fotografii sau pseudofotografii indecente; vezi, de asemenea, amănunte despre aceste reglementări în A. Murray, *op.cit.*, p. 372.

814 Vezi aplicarea în cazul R. v. Fellows & Arnold.

815 În USA, a fost dificilă aplicarea Child Pornography Act 1996, datorită prevederilor constituţionale referitoare la libertatea de expresie (First Amendment); vezi şi Free Sspeech

O variaţie interesantă în pseudoimaginile pornografice cu minori este un joc popular: *Online Age Play*. Acesta este o variaţie a unui fetiş sexual în care un partener joacă un rol de copil într-un scenariu. Problema principală este dacă acest tip de joc ar trebui să fie incriminat în conformitate cu legislaţia referitoare la abuzurilor comise asupra minorilor. În situaţiile în care *Online Age Play* este jucat de adulţi în casele lor este considerat un joc legal; dar dacă apelează la tehnologie digitală şi îl joacă în afară? Pentru a evita probleme de natură legală, furnizorii de servicii de la Second Life au declarat acest tip de activitate un joc interzis.

Un pericol deosebit privind imagini cu conţinut pornografic este reprezentat de folosirea reţele de socializare. Conform unui studiu realizat în Uniunea Europeană, 59% dintre minorii cu vârste între 9 şi 16 ani au profil pe o reţea de socializare (26% dintre aceştia fiind copii de 9-10 ani). În ceea ce priveşte ţările europene cu cel mai mare procentaj, Olanda este pe primul loc, cu 80%, urmată de Lituania, cu 76% şi Danemarca, cu 75% (România are un procent de 46% de copii care utilizează acest tip de reţele)[816].

În perioada 1 mai 2008 – 31 ianuarie 2009, Facebook a înlăturat peste 5.500 persoane condamnate pentru infracţiuni sexuale, iar MySpace a raportat înlăturarea a 90.000 persoane condamnate pentru infracţiuni sexuale în doi ani de pe site-ul său[817]. Cei în măsură să asigure siguranţa copiilor online încearcă să construiască strategii legislative şi tehnice care să maximizeze beneficiile acestui tip de comunicare şi să minimizeze riscurile de comitere a unor abuzuri. Statul Missouri din SUA a elaborat un act normativ în acest domeniu (Missouri Senate Bill 54), devenind primul stat care interzice profesorilor să fie "prieteni" cu elevii lor în cadrul tuturor reţelelor de socializare (este vorba numai de un contact direct), pentru a preveni *grooming*-ul[818] şi abuzuri mai grave asupra minorilor. Acest act normativ, care se mai numeşte şi „Amy Hestir Student Protection Act" (după numele unei eleve molestate şi hărţuite de profesorul ei o lungă perioadă de timp), a stârnit, cum era de aşteptat, controverse şi întrebări, legate de oportunitatea acestui tip de act, dar şi de unele greutăţi privind implementarea[819] (una din provocările pe care le semnalam la începutul acestei părţi: acest tip de tehnologie sofisticată face dificil un demers legislativ care să rezolve simplu o situaţie complexă).

Coalition (FSC) şi Prosecutorial Remedies and Other Tools to end the explotation of Children Today (PROTECT) Act 2003.

816 Vezi *EU Kids Online II: Enhancing Knowledge Regarding European Children's Use, Risk and Safety Online*, 2011, p. 36.

817 Vezi C. Chang, *Internet safety survey: Who will protect the children?*, Berkeley Technology Law Journal, Vol. 25, 2010.

818 Vezi Save the Children Europe Group, *Position Paper regarding online images of sexual abuse and other Internet-related sexual exploitation of Children*, updated August 2005, studiu disponibil la adresa http://www.savethechildren.it/2003/download/pubblicazioni/Stop-It/SC_Europe_Group_PositionPaper2005.pdf.

819 Vezi, pentru mai multe amănunte, http://newsfeed.time.com/2011/08/01/in-missouri-teachers-and-students-legally-cant-be-facebook-friends/#ixzz1Xvjj16GI.

Conţinut legal şi caracterizare

Cele două variante normative prevăzute de legiuitorul noului Cod penal, deşi sunt asemănătoare cu prevederile din art. 51 (1) al Legii nr. 161/2003, prezintă o resistematizare, o reformulare, dar şi o completare a calificării legale. Astfel, în art. 51 (1) al Legii nr. 161/2003 era reprodus integral textul art. 9 al Convenţiei europene privind criminalitatea informatică. Prin pornografia infantilă prin sisteme informatice, în definiţia dată de legiuitorul român în acest text, în vigoare până la intrarea în vigoare a noului Cod penal la 1 februarie 2014, se înţelegea producerea în vederea răspândirii, oferirea sau punerea la dispoziţie, răspândirea sau transmiterea, procurarea pentru sine sau pentru altul de materiale pornografice cu minori prin sisteme informatice ori deţinerea, fără drept, de materiale pornografice cu minori într-un sistem informatic sau un mijloc de stocare a datelor informatice. Această definiţie penală a încearcat să întărească măsurile de protecţie acordată minorilor, inclusiv protecţia lor împotriva exploatării sexuale[820], prin modernizarea dispoziţiilor penale pentru a circumscrie în mod efectiv utilizarea sistemelor informatice în comiterea pornografiei infantile.

Legiuitorul noului Cod penal a resistematizat textul, adăugând la agravanta din alin. 2 al art. 374 (*Pornografia infantilă*), o variantă atenuantă, care nu exista în legea nr. 161/2003 şi care priveşte, accesarea, fără drept, de materiale pornografice cu minori, prin intermediul sistemelor informatice sau altor mijloace de comunicaţii electronice (art. 374, alin. 3). Germenii prevederilor de acest tip au ca punct de plecare preocupările şefilor de stat şi de guvern, exprimate la cel de al doilea Summit (Strasbourg, 10-11 octombrie 1997) în Planul de acţiune şi corespunde unui curent internaţional care vizează interzicerea pornografiei infantile, curent evidenţiat inclusiv la nivelul Naţiunilor Unite[821]. Posesia (deţinerea) materialelor pornografice cu minori stimulează cererea de astfel de materiale, iar o cale efectivă de reducere a fenomenului constă în incriminarea oricărui comportament care constituie o etapă a lanţului dintre producţia de astfel de materiale şi posesia acestora[822].

---

820 Vezi în completare şi prevederile Legii nr. 678/2001 pentru prevenirea şi combaterea traficului de persoane, publicată în M. Of., nr. 783 din 11 decembrie 2001, modificată parţial prin Legea nr. 196/2003 privind prevenirea şi combaterea pornografiei.

821 Vezi *Optional Protocol to the UN Convention on the rights of the child, on the sale of children, child prostitution and child pornography*, precum şi Decizia Consiului UE nr. 375 privind combaterea pornografiei infantile prin Internet din 9 iunie 2000.

822 Doi tineri din Cluj-Napoca au fost trimişi în judecată pentru infracţiunea de pornografie infantilă prin intermediul sistemelor informatice, primul caz de acest gen aflat pe rolul Judecătoriei Cluj-Napoca. Astfel, în cursul anului 2005 şi la începutul anului 2006, cei doi tineri au deţinut şi pus la dispoziţie utilizatorilor din reţeaua la care erau abonaţi (*Internet Amnet Telecom*) filme pornografice cu minori. În urma percheziţiei efectuate, poliţiştii au descoperit în calculatoarele celor doi tineri zece filme pornografice cu minori, respectiv 17 astfel de filme (unele aparent realizate chiar în România), pe baza cărora au declanşat urmărirea penală împotriva celor doi sub acuzaţiile de deţinere şi răspândire de imagini pornografice cu minori – vezi pe larg articolul *Operaţiunea Lolita*, Clujeanul, 12-18 iunie 2006, p. 3.

BCU CLUJ / CENTRAL UNIVERSITY LIBRARY

Obiectul infracţiunii

Obiectul juridic special îl constituie relaţiile sociale privitoare la convieţuirea socială, în special la protecţia minorilor împotriva pornografiei infantile prin intermediul sistemelor informatice.

Obiectul material al infracţiunii poate fi suportul material (disc magnetic, dur etc.) folosit pentru stocarea datelor reprezentând materialele pornografice cu minori.

Subiecţii infracţiunii

a) Subiect activ al acestei infracţiuni poate fi orice persoană, fizică sau juridică, cu capacitate penală, textul neprevăzând nici o calitate specială pentru aceasta. *Participaţia penală* este posibilă sub toate formele (complicitate, coautorat, instigare).

b) Subiect pasiv general al infracţiunii este statul, iar **subiect pasiv special** este minorul a cărui exploatare sexuală se realizează prin activităţile incriminate în textul de lege.

Conţinut constitutiv

Latura obiectivă

Elementul material al laturii obiective în varianta agravată, prevăzută în art 374 alin. 2 noul Cod penal, constă în oricare din cele opt modalităţi alternative prevăzute de lege: *producerea, deţinerea în vederea expunerii sau distribuirii, achiziţionarea, stocarea, expunerea, promovarea, distribuirea, precum şi punerea la dispoziţie, în orice mod, de materiale pornografice cu minori, dacă au fost săvârşite printr-un sistem informatic sau alt mijloc de stocare a datelor informatice*; pentru varianta atenuată prevăzută la art. 374, alin. 3, este *accesarea, fără drept, de materiale pornografice cu minori, prin intermediul sistemelor informatice sau altor mijloace de comunicaţii electronice.* După cum se observă, faţă de varianta de bază prevăzută la art. 374, alin 1, la varianta agravată din alin. 2, cerinţa esenţială prevăzută pentru toate modalităţile normative enumerate este să fie *săvârşite printr-un sistem informatic sau alt mijloc de stocare a datelor informatice*, iar la cea atenuată (alin. 3) în plus faţă de această cerinţă esenţială, mai apare una: accesarea să se facă *fără drept*.

Prin "materiale pornografice cu minori", potrivit art. 374 alin. 4 noul Cod penal, se înţelege orice material care prezintă un minor având un comportament sexual explicit sau care, deşi nu prezintă o persoană reală, simulează, în mod credibil, un minor având un astfel de comportament. Această definiţie este uşor diferită de cea din art. 31 (1) lit. i din Legea nr. 161/2003, prin care se înţelegea orice material care prezintă un minor având un comportament sexual explicit sau o persoană majoră care este prezentată ca un minor având un comportament sexual explicit, ori imagini care, deşi nu prezintă o persoană reală, simulează, în mod credibil, un minor având un comportament sexual explicit.

Din modul în care legiuitorul a definit conceptul de "materiale pornografice cu minori", se observă înţelegerea şi exprimarea specificului acestor materiale în mediul digital. Astfel, în partea a doua a definiţiei, se arată că, deşi în material nu

prezintă o persoană reală, acesta simulează, în mod credibil, un minor având un comportament sexual explicit, aceste imagini putând fi opere digitale sub formă de înregistrări video, produse în scopul răspândirii, transmise, procurate, oferite sau puse la dispoziție ori deținute fără drept. De altfel, în Legea privind prevenirea și combaterea pornografiei (Legea nr. 196/2003), în art. 2, prin "materiale cu caracter obscen" (care includ și materiale pornografice cu minori), se înțeleg obiecte, gravuri, fotografii, holograme, desene, scrieri, imprimate, embleme, publicații, filme, înregistrări audio și video, spoturi publicitare, programe și aplicații informatice, piese muzicale, precum și orice alte forme de exprimare care prezintă explicit sau sugerează o activitate sexuală.

Trebuie reținut că ambele definiții prezentate mai sus se referă la o activitate sexuală sau un comportament sexual explicit. Prin urmare, poate fi reprezentat atât actul sexual, cât și orice altă atitudine sau poziție care poate fi considerată activitate sexuală sau un comportament sexual. După cum s-a precizat în literatura de specialitate, activitatea sexuală sau un comportamentul sexual reprezentate în aceste materiale pornografice cu minori trebuie să aibă caracter *explicit*[823]. Prin urmare, acesta trebuie să reiasă în mod direct din materialele respective, comportamentul minorului trebuie să fie evident, nu simple sugerări.

În Raportul explicativ privitor la Convenția europeană în domeniul criminalității informatice, la pct. 100, se arată că un "comportament sexual explicit" acoperă cel puțin următoarele, reale sau simulate:

- Raportul sexual, incluzând raportul genital-genital, genital-oral, anal-genital sau oral-anal între minori sau între un adult și un minor, de același sex sau de sex diferit;
- Bestialitatea (zoofilia);
- Masturbarea;
- Abuzul sadic sau masochist în context sexual;
- Expunerea lascivă a organelor genitale ale minorilor.

Dispozițiile art. 374 nu se aplică în cazul operelor de artă sau științifice, ori în cazul materialelor realizate în interes artistic, de cercetare, educației sau informare[824].

Prin "producerea în vederea distribuirii or expunerii" a materialelor pornografice se înțelege fabricarea, asamblarea, extragerea, combinarea unor asemenea materiale utilizând, în cele mai multe cazuri, instrumente sau tehnologii informatice. Cerința esențială în cazul acestei modalități normative este ca activitatea de producere a materialelor pornografice cu minori să se realizeze în vederea distribuirii comerciale sau expunerii. Dacă, spre exemplu, persoana care le-a produs nu a urmărit un asemenea scop (adică, nu a avut un scop lucrativ), va fi

---

823 Vezi M. Pătrăuș și C. Fl. Uzvat, *Pornografia infantilă în reglementările actuale*, Dreptul, 4, 38-52, 2003.

824 Vezi prevederile art. 3 alin. 1 și 2 din Legea nr. 196/2003 privind prevenirea și combaterea pornografiei; această precizare apare și în Raportul explicativ la Convenția europeană în domeniul criminalității informatice, pct. 99.

BCU IASI / CENTRAL UNIVERSITY LIBRARY

reţinută infracţiunea de pornografie infantilă prin intermediul sistemelor informatice, dar în varianta deţinerii unor asemenea materiale.

"Expunerea" materialelor cu minor presupune o participare "live", nefiind necesar ca activitatea să se întâmple într-un loc public sau deschis publicului, fiind, de fapt, chiar plauzibil ca astfel de activităţi să se desfăşoare într-un mediu privat[825]. Printre altele, nu este necesar ca expunerea să aibă loc prin prezentare unui "public", adică mai multor persoane, putând fi destinată unei anumite "clientele"[826].

"Distribuirea" se referă la activitatea de difuzare a materialelor pornografice cu minori, iar "transmiterea" este activitatea de diseminare activă a materialelor pornografice cu minori (astfel, transmiterea de materiale pornografice cu minori printr-un sistem informatic către o altă persoană, îndeplineşte condiţiile pentru a fi considerată în cadrul acestei infracţiuni). Prin "stocare" înţelege copierea pe un dispozitiv pentru păstrarea datelor informatice pe perioade indefinite (cum ar fi, spre exemplu, un disc dur sau o cheie USB).

Prin "punere la dispoziţie" se înţelege întreaga gamă de activităţi prin care se asigură accesul, gratuit sau contra cost, la asemenea materiale. În esenţă, punerea la dispoziţie de materiale pornografice cu minori se realizează prin plasarea materialelor online (spre exemplu, pe un site web) sau prin crearea de legături *hypertext* la pagini web care conţin astfel de materiale, pentru a facilita accesul. Prin "achiziţionare" se înţelege activitatea de obţinere de materiale pornografice cu minori prin intermediul sistemelor informatice, prin descărcare digitală (*download*).

Legiuitorul penal prevede variante alternative, la care adaugă sintagma "în orice mod", ceea ce înseamnă că alte modalităţi de comitere (închiriere, oferire gratuită etc.) sunt posibile. Trebuie precizat că nu orice material pornografic produs pentru răspândire, oferit, transmis, deţinut etc. prin intermediul sistemelor informatice îndeplineşte condiţiile stabilite de art. 374 noul Cod penal, ci doar materialele pronografice cu *minori*. Prin "minor" se înţelege persoana care are mai puţin de 18 ani, în acord cu definiţia dată de Naţiunile Unite termenului "copil" în Convenţia Naţiunilor Unite privind drepturile copilului.

Prin "accesare" (varianta atenuată de la art. 374, alin. 3) se înţelege contactul cu aceste materialee prin intermediul sistemelor informatice sau a altor mijloace de comunicaţie electronică. Prin urmare, legea română pedepseşte nu numai crearea de site-uri de pornografie infantilă, ci şi accesarea lor. La această variantă este prevăzută cerinţa esenţială "fără drept".

Urmarea socialmente periculoasă este reprezentată de producerea unei stări de pericol cu privire la moralitatea şi decenţa minorilor. Aceasta se produce în momentul în care se realizează oricare din activităţile incriminate în textul de lege.

Raportul de cauzalitate rezultă *ex re*, adică din materialitatea faptei.

Latura subiectivă

Sub aspectul vinovăţiei, fapta se realizează cu intenţie directă sau indirectă.

---

825 Luigi Delpino, *Diritto penale - Parte speciale*, Ed. Simone, Italia, 2004, p. 564.
826 *Id.*

Formele infracțiunii

Tentativa este posibilă și este pedepsită (conform alin. 5, art. 374 C. pen.).

Epuizarea infracțiunii are loc în momentul realizării ultimului act incriminat de legiuitor. Infracțiunea se poate prezenta și în forma continuată.

Sancțiunea

Pedeapsa prevăzută de lege pentru varianta agravată de la art. 374, alin. 2 este închisoare de la 2 la 7 ani, iar pentru cea atenuată de la alin. 3 este închisoare de la 3 luni la 3 ani sau amendă (pedeapsa a fost redusă față de cea prevăzută de art. 51 din Legea nr. 161/2003, care era închisoare de la 3 la 12 ani).

BCU IASI/CENTRAL UNIVERSITY LIBRARY

B.C.U. "M. EMINESCU" IAȘI

BCU IASI/CENTRAL UNIVERSITY LIBRARY

B.C.U. „M. EMINESCU" IAŞI

BCU IASI/CENTRAL UNIVERSITY LIBRARY

DREPTUL TEHNOLOGIEI INFORMAȚIILOR ȘI COMUNICAȚIILOR

A 98

Această carte cuprinde o analiză comprehensivă a problemelor legale apărute în epoca digitală şi se adresează profesioniştilor şi studenţilor din domeniile juridic şi cel al afacerilor. În cadrul studiului, sunt discutate aspecte teoretice şi practice esenţiale privind afacerile electronice, drepturile de proprietate intelectuală în cyberspaţiu şi infracţiunile informatice, incluzând prezentarea legislaţiei naţionale în domeniu, precum şi numeroase referinţe la dreptul, doctrina şi jurisprudenţa altor state.

editura Albastră
400500 str. Observatorului 1
Cluj-Napoca, România
tel. 0264.438328*, fax 0264.438330
e-mail:albastra@gmi.ro

librăria virtuală
www.albastra.ro
www.gmi.ro

I.S.B.N. 978-973-650-306-1

editura Albastră

BCU IASI/CENTRAL UNIVERSITY LIBRARY